Enterprise Networks

Welcome to Enterprise Solutions Training

0365 Voice Over Internet Protocol Technologies

Student Guide

© 2002-2003 Nortel Networks Corporation.

All rights reserved.

Information in this document is subject to change without notice. Nortel Networks Corporation assumes no responsibility for any errors that may appear in this document. Neither this document nor any portion thereof is to be reproduced in any form without the written permission of Enterprise Solutions Training, Nortel Networks Corporation.

NORTEL, NORTEL NETWORKS, the NORTEL NETWORKS corporate logo, the globe mark design, NORTEL NETWORKS How the world shares ideas, Meridian, and Succession Communication Server for Enterprise 1000 are trademarks of Nortel Networks Corporation. All other trademarks are the property of their owners.

Welcome Template.FM Issue 3.0 July 19, 1999 Training Design

NORTEL NETWORKS

Revision History

January 6, 2003

Up-issued to replace 0927C.

September 30, 2002

0927C controlled release.

Welcome

Introduction

Audience

This course is designed for Sales or System Engineers, Technical Support Specialists, and Installation Specialists with a working knowledge of voice and data who need the fundamentals of Voice over Internet Protocol (VoIP) technologies, including:

- Voice packetization
- Packet telephony design issues
- Traffic convergence issues
- VoIP standardization and protocols
- Network assessment

Background

This course was designed to to help participants prepare to take the Nortel Networks 801 VoIP Technology Exam (Number: 921-801).

Notes

Objective

After completing this course, you will be able to:

- Describe how to packetize voice using voice packet analysis, compression standards, Real Time Protocol (RTP), and User Datagram Protocol (UDP)
- Explain and differentiate between the major components of Voice over Internet Protocol (VoIP)
- Define voice quality on a data network, including the performance of speech CODECs, delay, echo impairment and control, and packet loss
- Given required voice CODEC, voice payload, and link speed, calculate the bandwidth requirements for VoIP network engineering
- Describe the common models for voice quality, including E-Model G.107 and Mean Opinion Score (MOS)
- Define methods available for implementing QoS including Resource ReSerVation Protocol (IS/RSVP) Approach, Differentiated Services (DiffServ) Approach, and Ethernet 802 standards
- Identify the challenges of low speed Wide Area Network (WAN) connections focusing on serialization delay and Maximum Transmission Unit (MTU)
- Define the network infrastructure, including the LAN/WAN environment and Security issues
- Describe the components of the H.323 standard, including the terminal, gateway, gatekeeper, and Multipoint Control Unit (MCU)
- Identify the Session Initiation Protocol (SIP) objectives and protocol
- Explain the differences between the SIP and H.323 standards
- Given sample network assessment scenarios, determine the network assessment steps and tools for customer network improvements

Notes

Contents

Notes

NNCSS
801
VoIP

http://www.nortelnetworks.com/servsup/tc/

Notes

How it Works

Introduction

In the area of communications, convergence refers to the act of bringing voice and data services together to form a united system with common cabling, equipment, and management.

On a converged network, voice traffic is transported over the IP network, rather than the traditional Public Switched Telephony Network (PSTN). Using IP, calls travel as packets of data on shared lines at a much faster rate and utilize less equipment, while avoiding PSTN charge.

This lesson reviews some communication fundamentals. For additional information about these concepts, see the *Voice Fundamentals Reference Guide*, which is packaged with your course materials.

Notes

Objectives

Given this module and the instructor's presentation, you will be able to communicate about communication fundamentals, such as:

- Analog-to-Digital Conversion
- Pulse Code Modulation
- Circuit Switching
- Packet Switching
- Time Division Multiplexing
- T-1 Connections
- Integrated Services Digital Network
- Frame Relay
- Asynchronous Transfer Mode
- Internet Protocol Network
- How VoIP Works
- Signaling System 7
- Synchronous Optical Network
- Network Performance

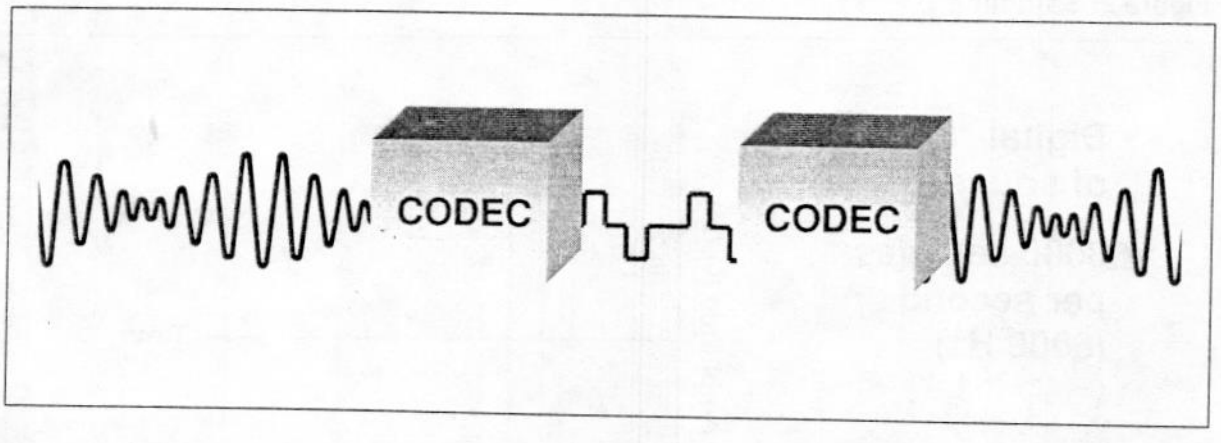
Notes

Analog-to-Digital Conversion

As information is presented in analog format, conversion to digital occurs at various points during transmission through the use of a CODEC (coder/decoder), which can be located in the telephone instrument, the Private Branch Exchange (PBX), or the Central Office (CO) equipment.

When the digital signal arrives at its destination, it is then converted back to analog (through a CODEC) for the user to understand.

Figure 1: Analog-to-Digital Conversion



Voice 300 Hz - 4000 Hz
× 2
8 KHz

1 sec / 8000
= 125 μsec.

Notes

LAN 64K G.711 μ-law
WAN 8K G.729 A/B
6.3K
5.3K G.723.1

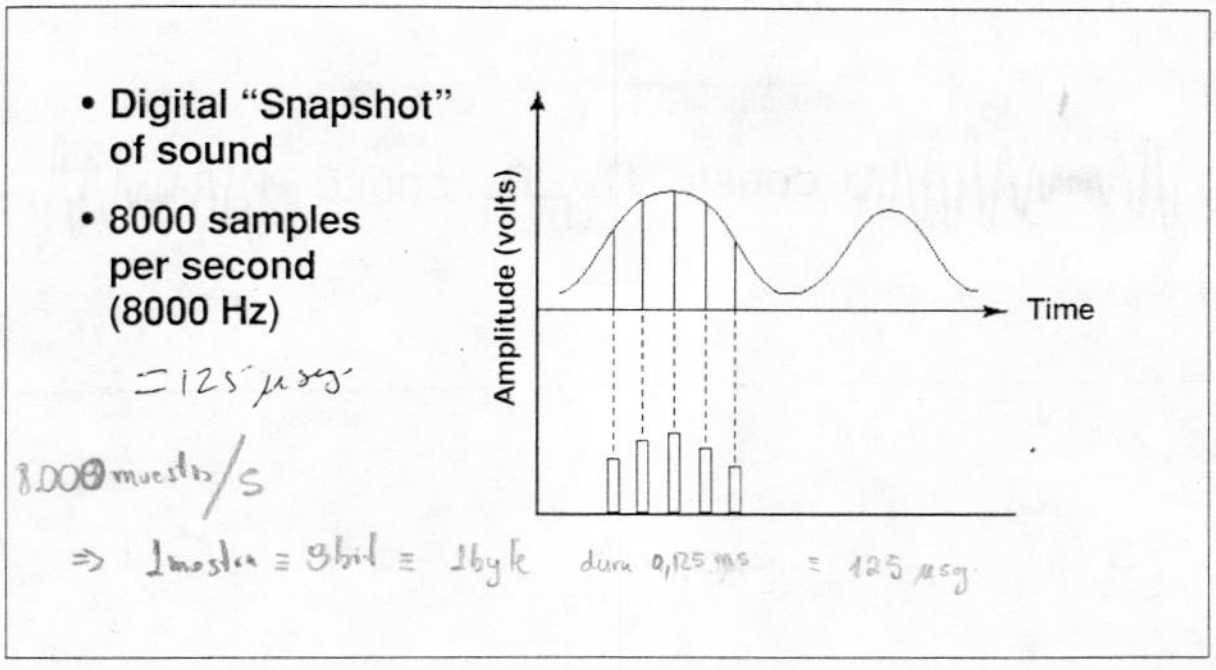
Pulse Code Modulation

During the analog to digital conversion, an analog signal undergoes a series of steps.

Sampling

Pulse Code Modulation (PCM) is the process used for sampling. PCM assigns an 8-bit binary code (1 or 0) to a specific amplitude of a signal. Sounds are sampled at eight thousand samples per second. The sampling rate must be at least twice the maximum frequency of the signal being sampled.

Figure 2: Sampling

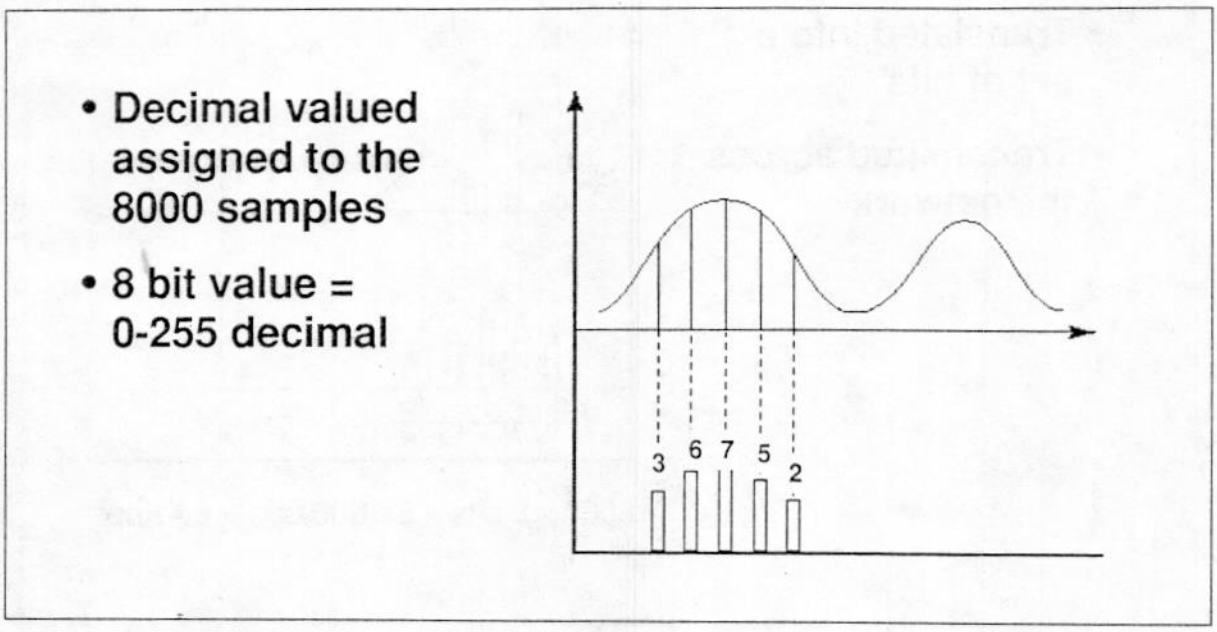


Notes

Quantization

Once sampling has occurred, the "snapshot" is quantized and assigned a number. During quantization, companding can occur when a voice is too loud or too soft. Companding allows a soft signal to be measured with the same degree of accuracy as the loud signal.

Figure 3: Quantization

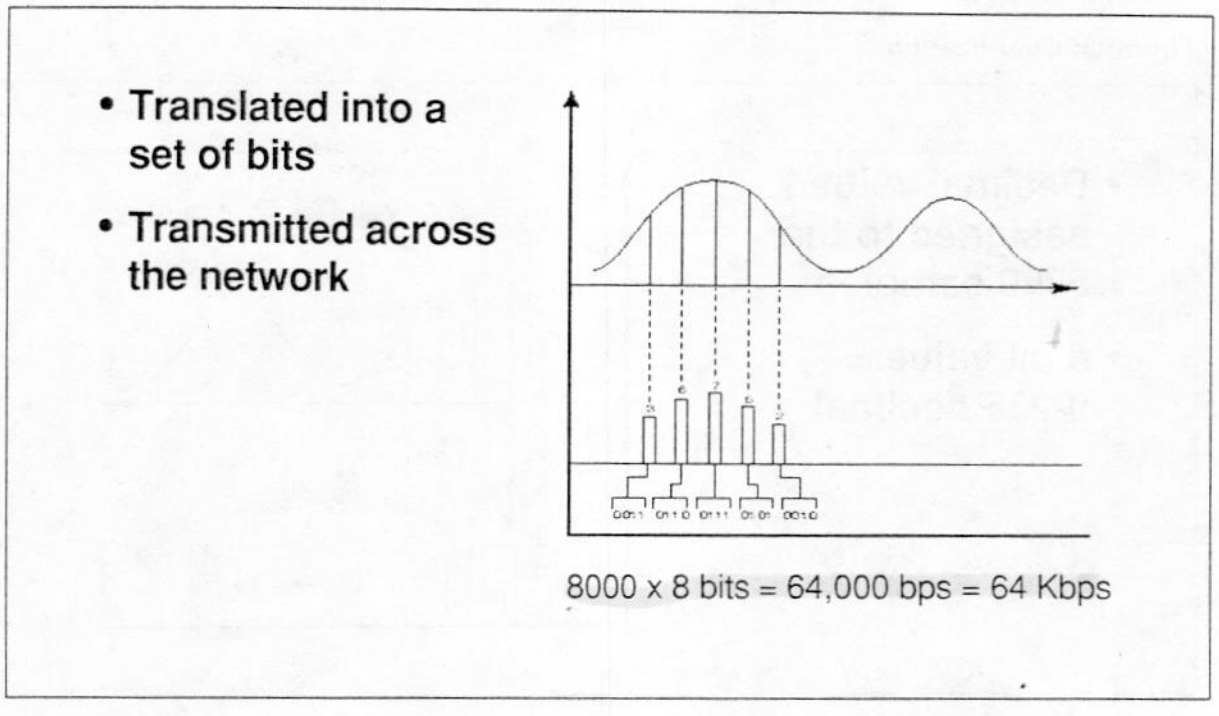


Notes

Coding

Each quantized signal is coded, translated into a set of bits, and transmitted across the network.

Figure 4: Coding



Because these separate "snapshots" are transmitted so closely together, these "snapshots" can run together and create the effect of continuous sound, the way a movie's many frames of film create the illusion of motion

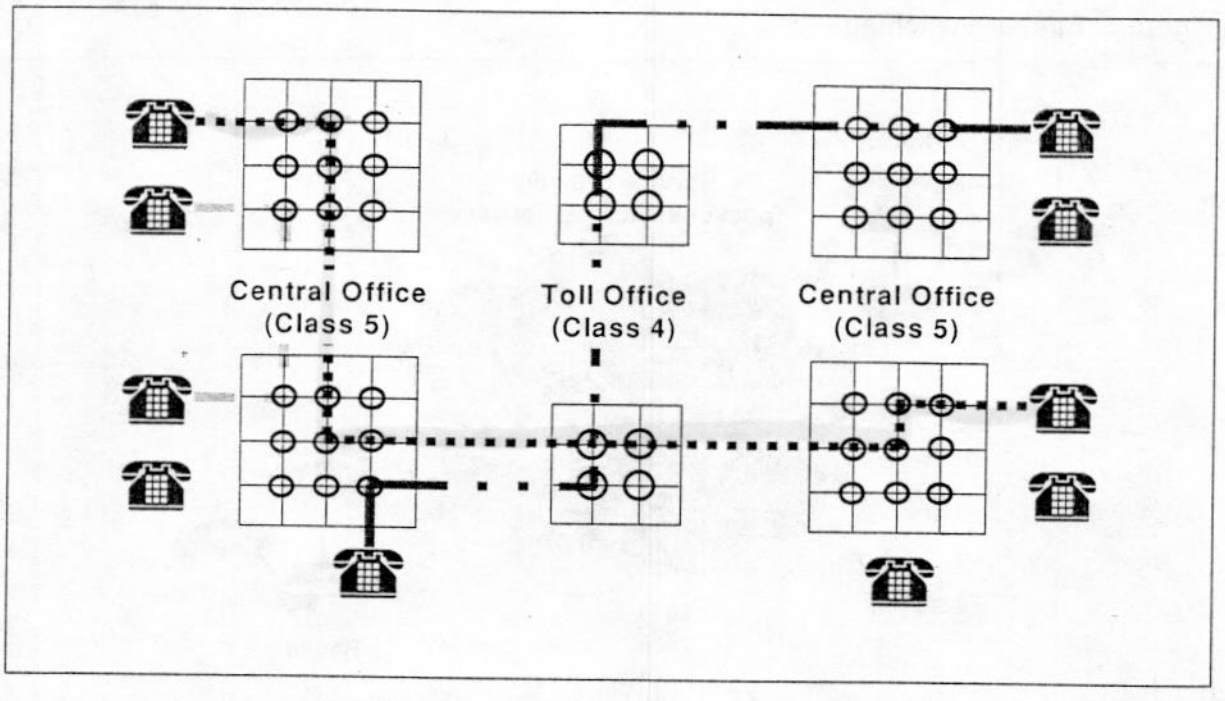
Notes

Circuit Switching

A circuit-switched network establishes a dedicated circuit between two locations during the entire call setup, until disconnect occurs. Information, including silent pauses, is transmitted in a continuous stream. A phone connection is generally a circuit-switched network. If information is sensitive to delay, such as voice and video applications, circuit-switching is best. However, it can be quite expensive, since equipment is dedicated solely for a particular call.

The figure below shows how circuit switching provides dedicated connections for the duration of each call.

Figure 5: Circuit Switching



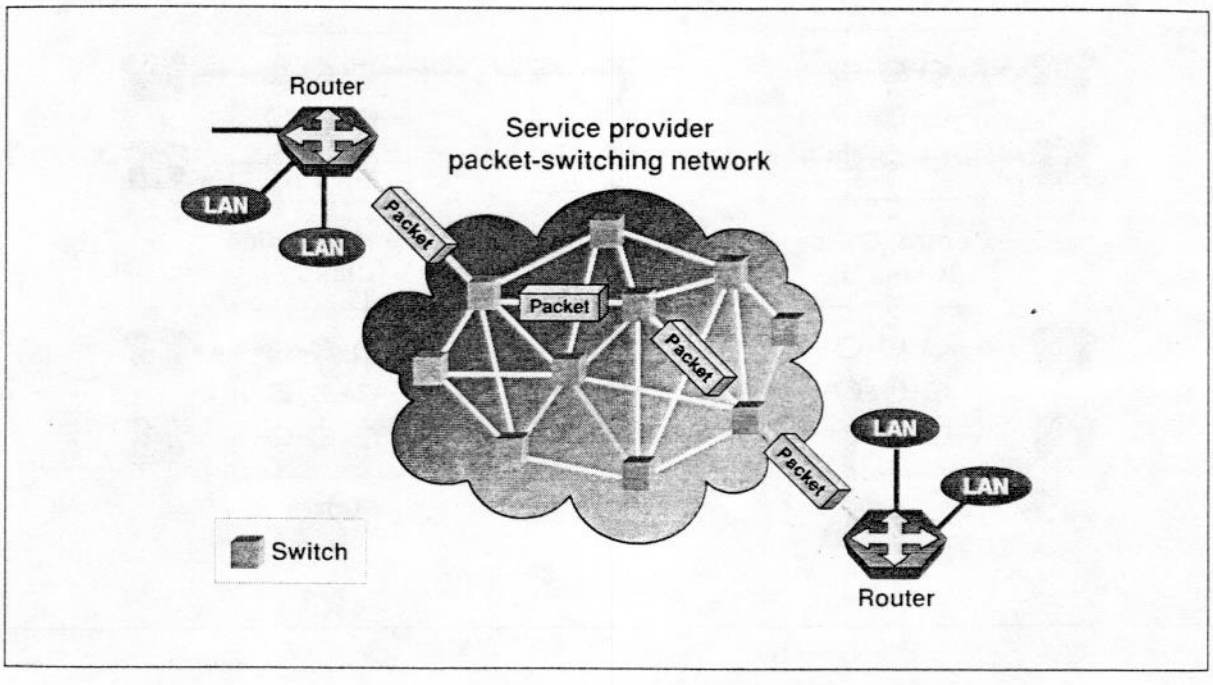
Notes

Packet Switching

Data packets of various sizes are routed and relayed in a packet-switched network. Each data packet is transmitted separately over individual circuits and reconverted into data at the destination. Each circuit is in use only for transmission of data packets, and then the circuit is released. If a pause or silence occurs during transmission, circuits are not used. When data packets begin transmitting again, another circuit relays the data. At the destination, all packets with similar headers are grouped together, organized, and delivered. A Frame Relay WAN is a packet-switched network, since this type of traffic can withstand delays and jitter and can transmit bursts of data.

The figure below shows how packet switching sends information over the same path.

Figure 6: Packet Switching



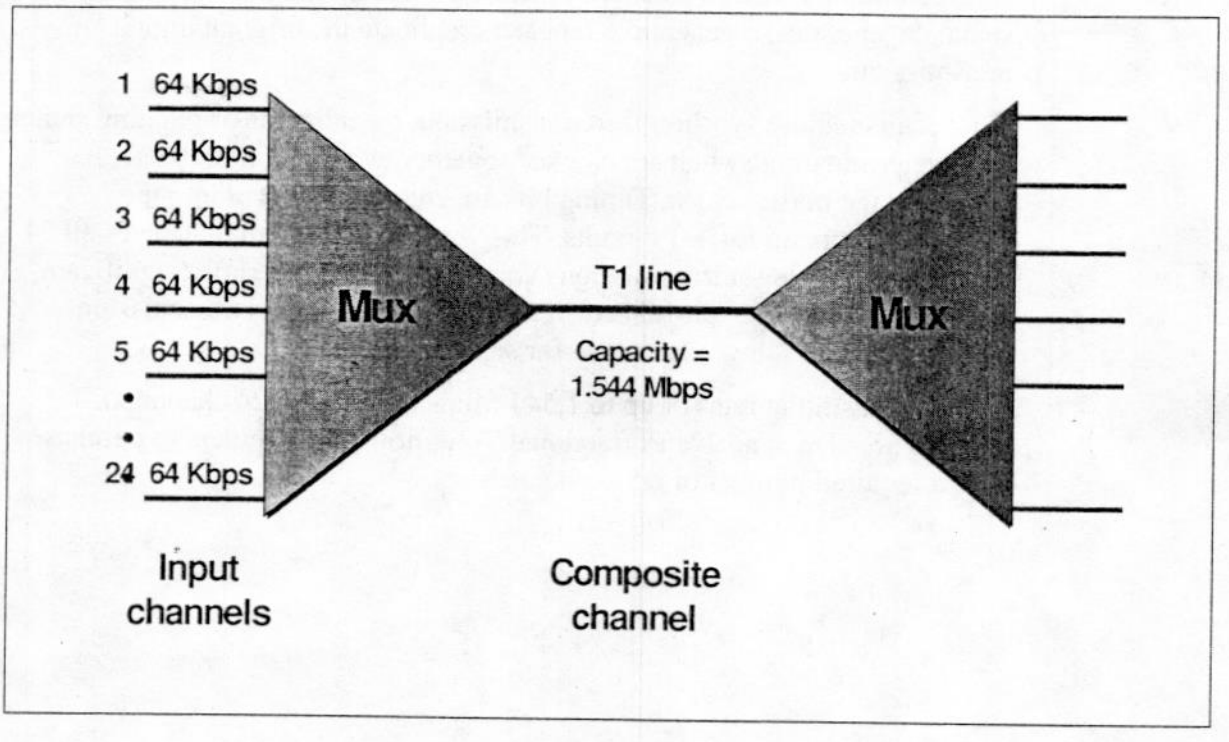
Notes

Time Division Multiplexing

Time Division Multiplexing (TDM) is a common transmission path shared by a number of channels on a recurring basis, interleaving data onto DS-0 channels.

TDM supports awide variety of services and technologies, such as video, data, Frame Relay, LAN/WAN, ISDN, and ATM.

Figure 7: Time Division Multiplexing



Notes

T-1 Connections

A T-1 provides up to 24 channels of service between two switches, or a switch and a CO, over four pair of wires. Before the T-1, 24 conversations required 24 separate pairs of wire. Those 24 wires are now the size of a regular telephone cord. A T-1 circuit increases a telecommunications network backbone without proportionally increasing the amount of wiring and equipment.

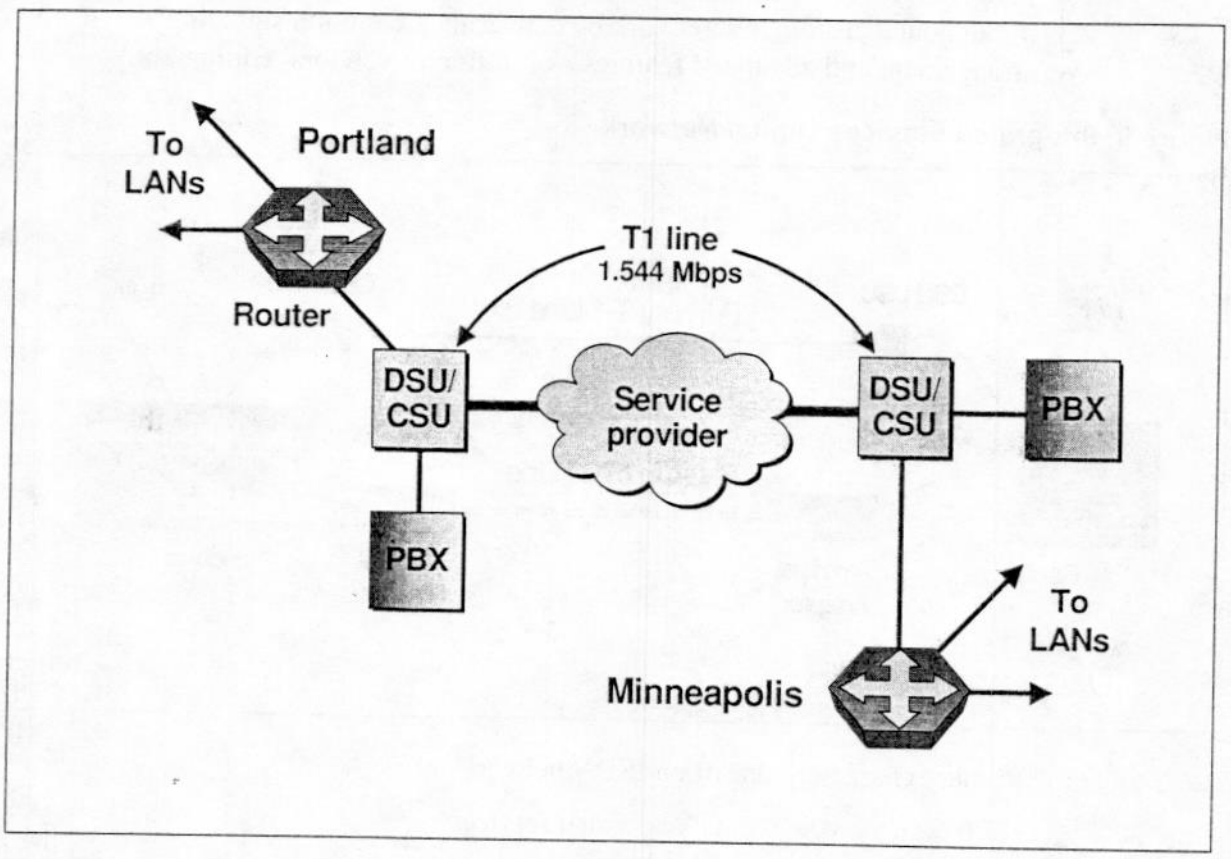
T-1 services are digital, with information configured as 1s and 0s. This configuration provides a cleaner transmission and minimizes noise. When a signal degenerates, regenerative repeaters replicate the original digital transmission.

T-1 circuits require synchronized transmission, meaning the originating switch and the terminating switch are clocked together, with the primary site providing the master clock. Timing bits are encoded and sent into the information stream for T-1 circuits. This "bit-robbed signaling" leaves all 24 channels available for transmission. Voice services do not suffer significant degradation from the "bit-robbed signaling;" however, data transmission occurs at 56K to allow extra room for signaling.

T-1 can transmit at rates of up to 1.544 Mbps (64 Kbps x 24 channels). T-1 services are also available as fractional T-1, allowing customers to purchase only a required number of DS-0 channels.

Notes

Figure 8: T-1 Connections

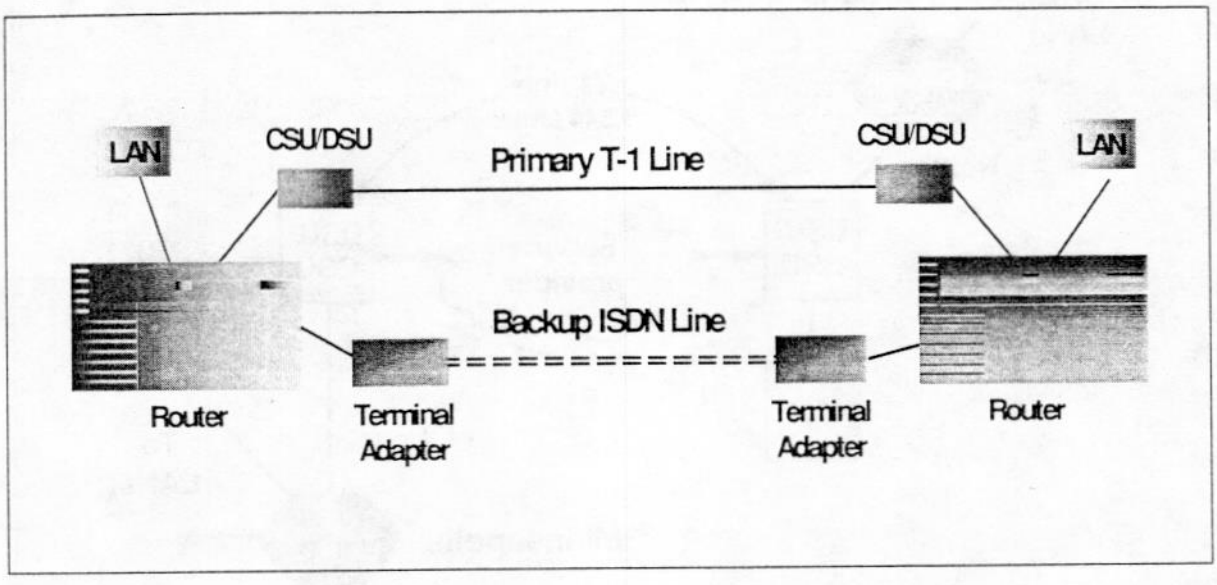


Notes

Integrated Services Digital Network

Integrated Services Digital Network (ISDN) provides PBX-like services throughout a customer's network by delivering a common signaling arrangement and advanced features over different vendors' equipment.

Figure 9: Integrated Services Digital Network



Primary characteristics of an ISDN network are:

- Integrates voice, data, and video services
- Has a digital end-to-end connection that provides high transmission quality
- Has improved and expanded services because of B- and D-channel data rates
- Is more efficient and productive
- Offers advances in device connectivity

Notes

Two popular ISDN services are:

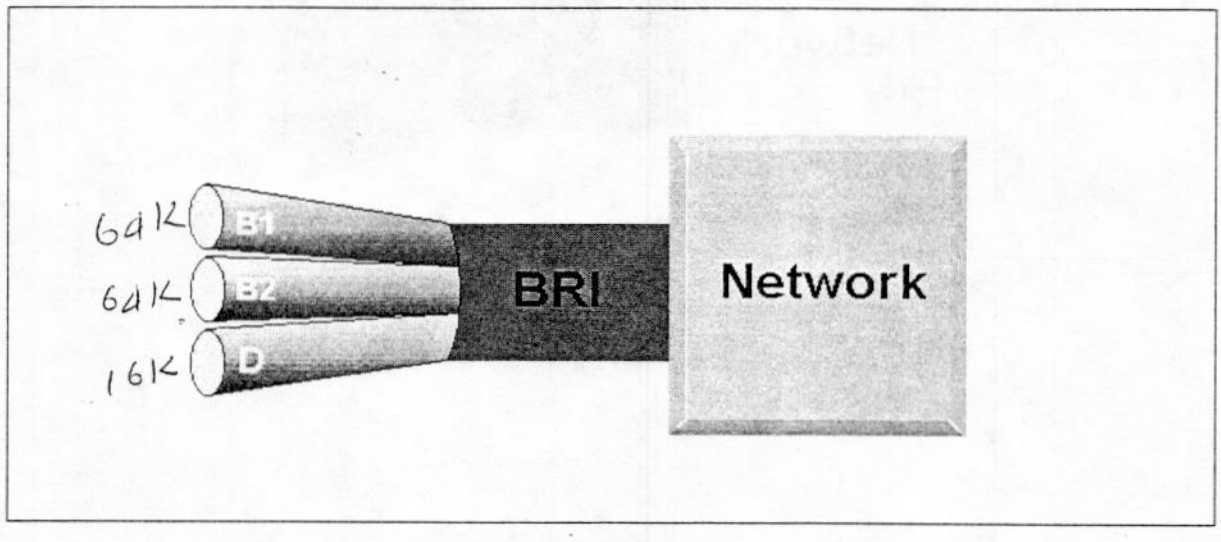
- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

Basic Rate Interface

BRI integrates voice and data requirements, primarily for home office environments, using existing copper wire.

BRI provides up to 128 Kbps transmission capability with the ability to have simultaneous multiple devices active over two B+D channels. BRI allows a user to be on the Internet while receiving a fax transmission, since neither device uses the entire bandwidth.

Figure 10: Basic Rate Interface



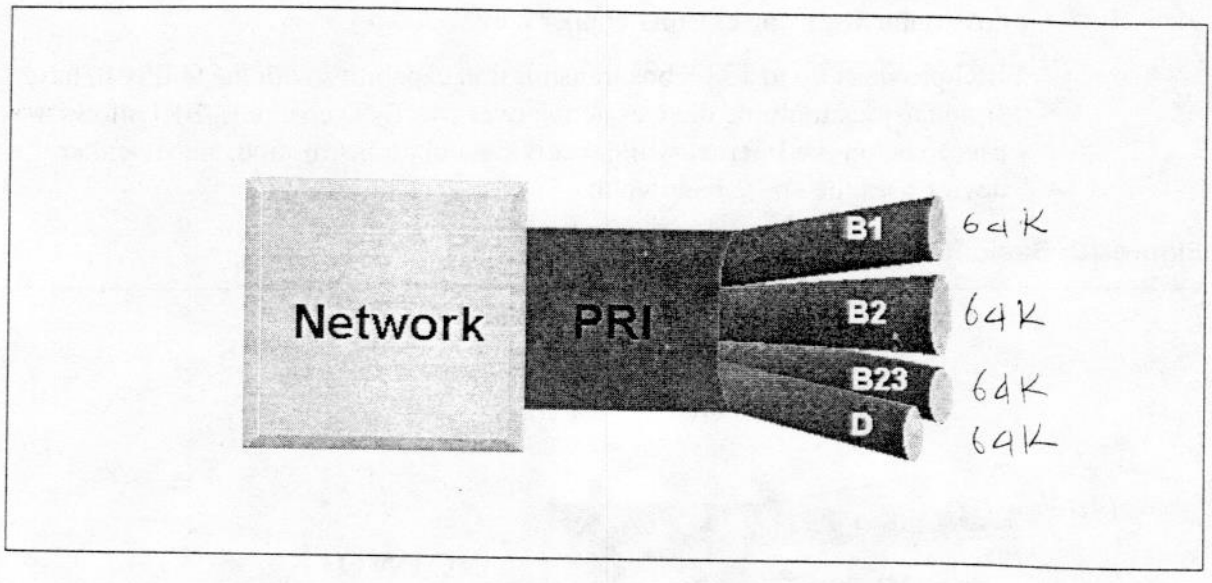
Notes

Primary Rate Interface

PRI is designed for corporate networks requiring T-1 and integrated voice and data capability.

PRI provides up to 1.54 Mbps transmission capability through 23 B+D channels while enhancing signaling and transmission capabilities.

Figure 11: Primary Rate Interface



Notes

Frame Relay

Originally defined for use over ISDN, Frame Relay (FR) is a fast packet-switching technology for transporting data in both private and public networks. FR provides data speeds between 56 Kbps and 45 Mbps. It offers greater efficiencies and speed of operation, though no error protection in transporting data is available. If frames of data are corrupted while transported, they are discarded. It is the responsibility of the end devices to identify data loss and attempt to initiate recovery by retransmitting the frame of data.

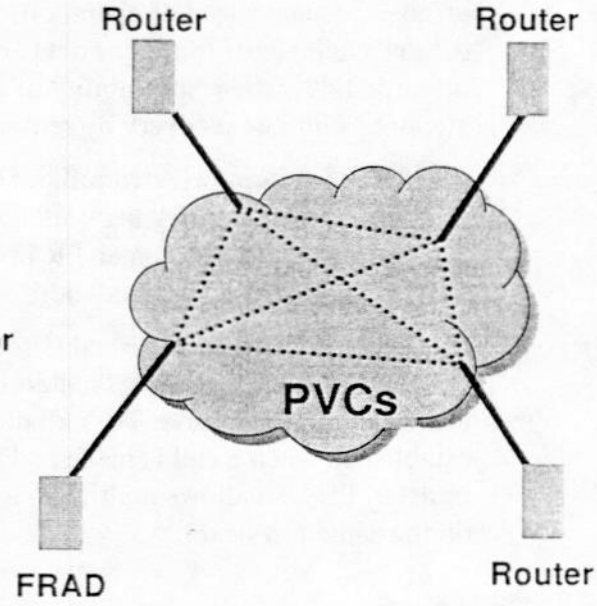
FR is a connection-oriented protocol. A communications path must be established on a network between a source and destination before data frames can be sent. Bandwidth on an FR link is used only when traffic is sent. If no traffic is being sent, the bandwidth on the link is potentially available for use.

FR supports Permanent Virtual Circuits (PVC) and Switched Virtual Circuits (SVC). PVCs are generally "nailed-up" circuits. Once established, they are always available for use. The call destination never varies. SVCs are established when a call is made and last only for the duration of the data transfer. FR also allows multiple Virtual Circuits (VC) data to be transmitted on the same physical link.

Notes

Figure 12: Frame Relay

- T-carrier on steroids
- 1.544 Mbps without the T-carrier overhead
- Does not check for errors
- Connections are PVC (Private Virtual Circuits) or SVC (Switched Virtual Circuits)
- Allows high speed; low delays
- Ideal for large corporate networks



Notes

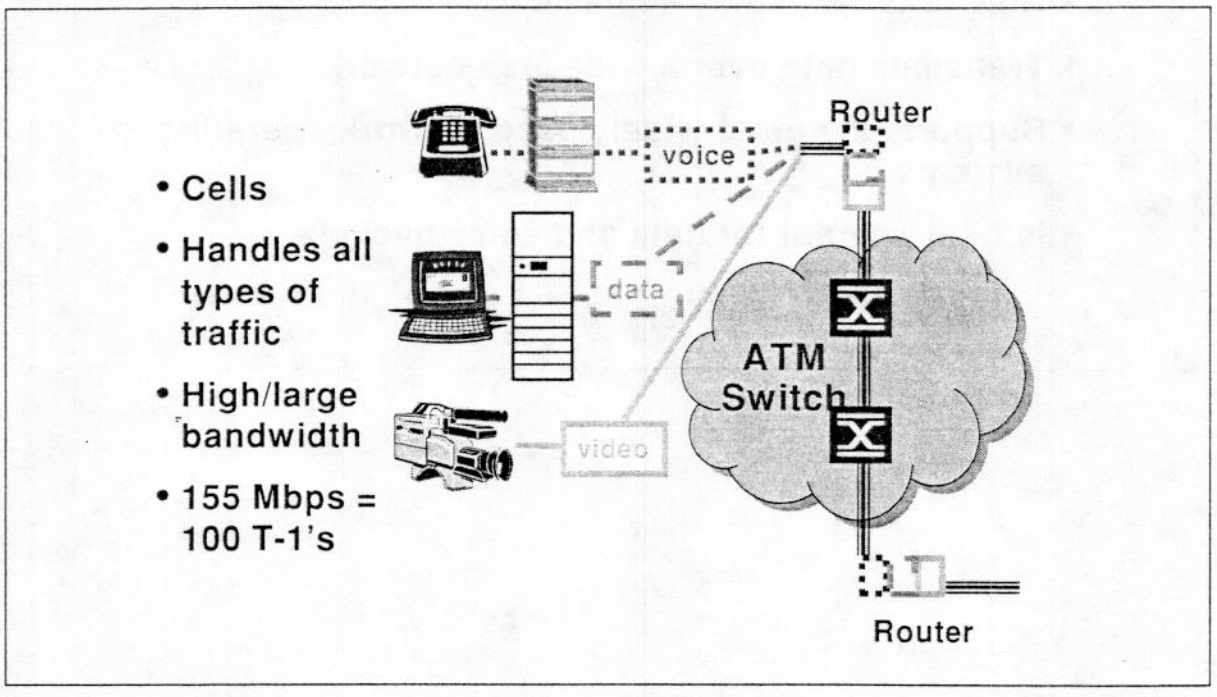
Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a combination of circuit- and packet-switching technology using high speed transmission, high bandwidth and low delay techniques.

ATM sends data only when needed. It requires that network connections are in place before transmission can occur.

ATM utilizes fixed-length, 53-byte packets, called cells, for transporting traffic over the network. ATM also balances shorter cells for delay-sensitive traffic, such as voice and video, and longer cells for delay-tolerant traffic, such as data.

Figure 13: Asynchronous Transfer Mode



Notes

Internet Protocol Network

The Internet Protocol (IP) is a highly flexible, scalable protocol that transmits information across any network.

Figure 14: Internet Protocol Network

- Most flexible networking protocol in use today for telephony solutions in Wide Area Networks (WAN), Local Area Networks (LAN), and applications
- Networks are highly scalable
- Transmits data over a wide area network
- Supports the most widely used network operating systems
- Is fault tolerant for data and voice packets

Notes

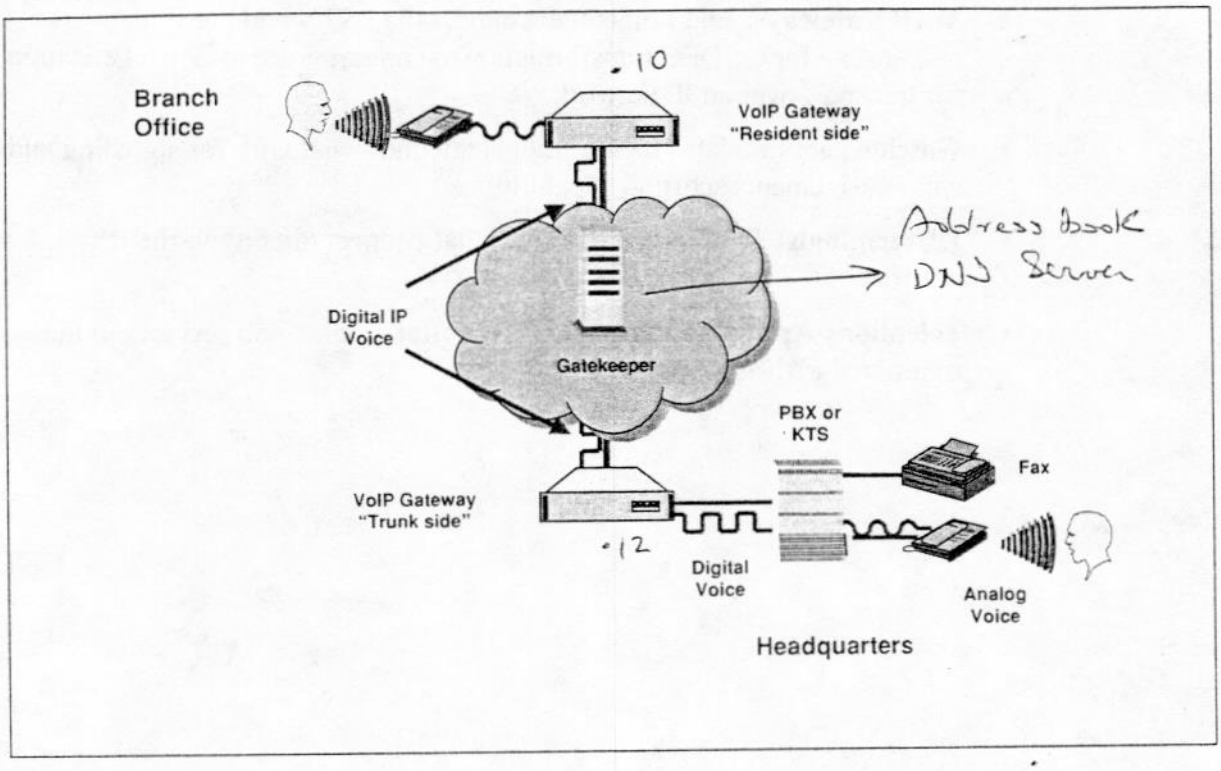
How VoIP Works

There are four components to IP Telephony:

- **VoIP Gateways:** End-points that connect the PSTN and the IP network; responsible for CODEC transformation to convert voice to IP packetization for transport over an IP network
- **Gatekeeper:** Emulates the traditional telephony network for signaling and call management reporting capability
- **IP Terminals:** Telephony end-points that connect directly to the IP network
- **Telephony Applications:** Enable IP to offer feature-rich services in the traditional PBX environment

Notes

Figure 15: How VoIP Works



Notes

Signaling System 7

Signaling System 7 (SS7) is the backbone of the current communications network. SS7 utilizes digital signaling in a circuit-switched network with a separate packet network to set up calls, which frees up voice and data trunks to carry their optimal amount of traffic.

SS7 is considered a smart network because it sets up and tears down calls and also supports Advanced Intelligent Network (AIN), where a user dials a national telephone number and the call is routed to the closest branch location.

S7 uses out-of-band signaling, or signaling is transmitted by a facility separate from the one carrying traffic. Calls are set up faster and sophisticated service options, such as 800 number service, CLASS features and calling card verification, are available. SS7 enhances ISDN capability, which allows ISDN networking across an entire network.

Notes

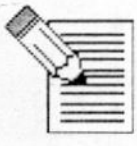
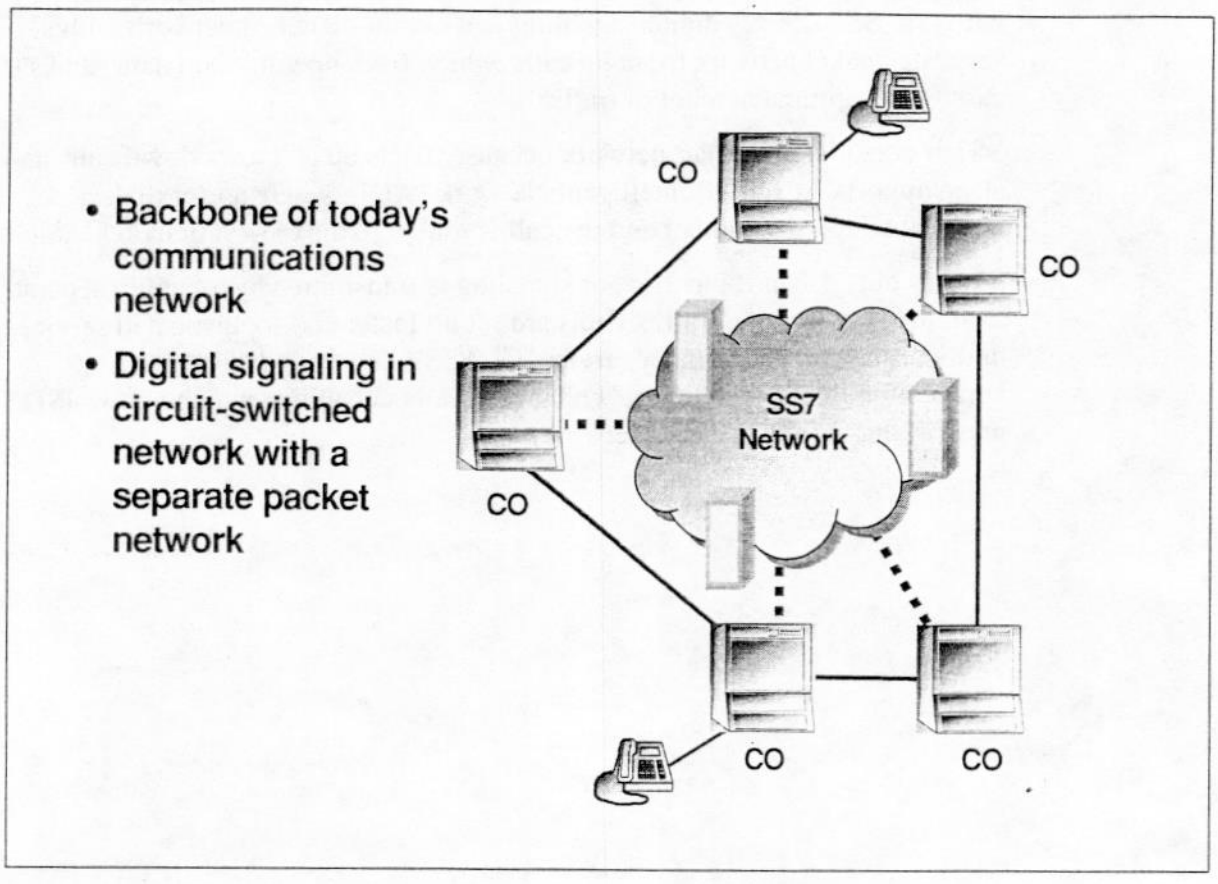


Figure 16: Signaling System 7



Notes

Synchronous Optical Network

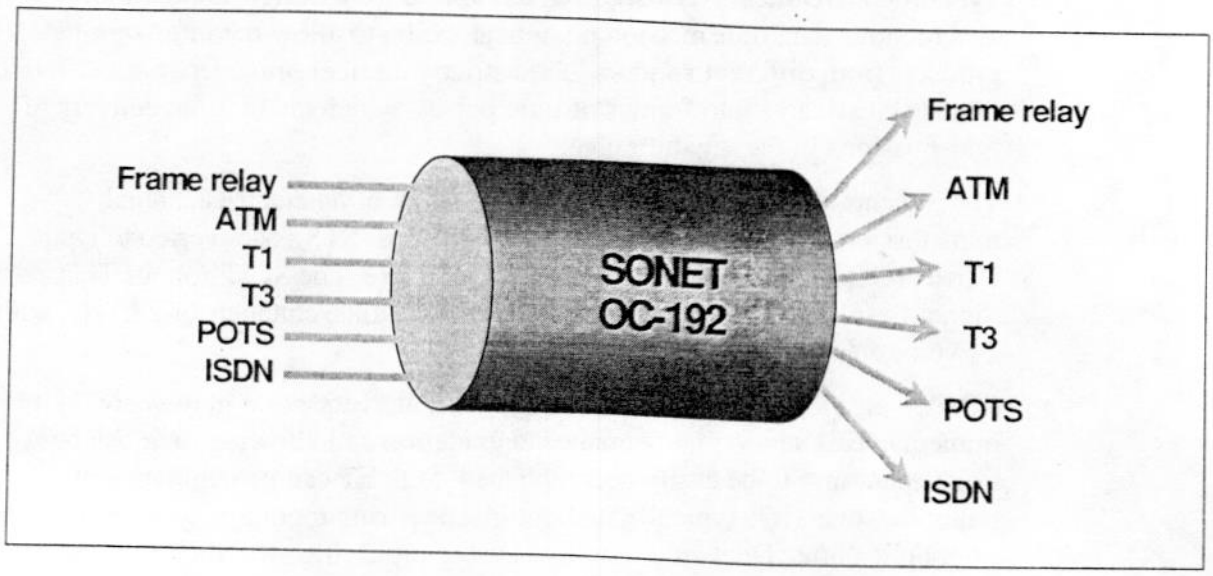
Synchronous Optical Network (SONET) provides a design standard for synchronous data transmission on optical media to allow the interworking of products from different vendors. Used strictly on fiber optic networks, SONET divides bit streams into frames of light pulses, which enables the delivery of transmissions in the gigabit range.

The Synchronous Transport Signal (STS) is the basic electrical signal transmission rate and has a speed of 51.84 Mbps. STS is converted to Optical Carrier (OC-1), the basic optical transmission rate. The Synchronous Transport Signal Level 1 (STS-1) has the capacity of 672 voice channels or 28 T-1s, with 24 voice channels.

SONET provides performance measurement at every point in the network by immediately detecting performance degradation and allowing maintenance troubleshooting to be easily accomplished. SONET can be deployed point-to-point; however, it is typically laid out in a dual-ring topology, with redundant fiber optic paths. Dual-ring topology causes rapid ring switching to occur in the event of fiber or equipment failures, which drastically improves the survivability of the network.

Notes

Figure 17: Synchronous Optical Network



Notes

Network Performance

In the world of voice communications, the goal is to provide 99.999% reliability. This high level of reliability requires constant performance monitoring and error checking by both access and network equipment. Factors such as jitter, delay, distortion, and echo can immediately denigrate network performance.

In the lessons that follow, you will learn about the methods that you can use to implement Quality of Service and reliability.

Figure 18: Network Performance

- **Goal is to provide 99.999% on-line reliability, cornerstone of circuit-switching network**
- **Requires constant performance monitoring and error checking**
- **Factors which can adversely affect network performance**
  - Jitter: End result is jitter pops and clicks (variable delay only)
  - Delay: End result in voice transmission is echo; in data transmission end result is distortion of data
  - Distortion: Direct result of compressing voice at a rate of less than 64 Kbps
  - Echo: Result of several factions such as strength of the speech returned, Round-trip Delay (RTD) and Echo Return Loss (ERL)
  - Lost packets

Notes

Summary

In lesson, you reviewed communication fundamentals, such as:

- Analog-to-Digital Conversion
- Pulse Code Modulation
- Circuit Switching
- Packet Switching
- Time Division Multiplexing
- T-1 Connections
- Integrated Services Digital Network
- Frame Relay
- Asynchronous Transfer Mode
- Internet Protocol Network
- How VoIP Works
- Signaling System 7
- Synchronous Optical Network
- Network Performance

Notes

Packet Telephony Overview

Introduction

Convergence of the telephone network and the Internet is driving the use of packet-based transmission for telecommunications networks. Integration of voice and data onto a single network offers significantly improved efficiency for both private and public network operators. Data is carried most efficiently on packet networks.

Because data has overtaken voice as the major type of telecom traffic, and data traffic volume continues to grow faster than voice traffic volume, it is not surprising that the integrated network uses packet-based transmission. Packet-based transmission of digital voice is a logical step, but it has some important implications for voice quality:

- Network design, such as packet sizes, packet header overhead, and the sizes of queues and buffers, was chosen for optimal efficiency of data transfer.
- Access links, which are dedicated to voice in switched-circuit networks, can be shared between voice and data in the packet environment.

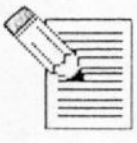
Notes

Objectives

Given this module and the instructor's presentation, you will be able to:

- Apply knowledge of how voice is sampled and converted into IP packets to calculate overhead
- Compare and contrast Voice over IP packet-switching models
- Calculate bandwidth for different compression standards based upon voice samples in milliseconds (ms)
- Apply knowledge of the attributes of Real-Time Protocol (RTP) to identify why it is ideal for handling packetized voice in an IP telephony environment
- Compare the unique attributes of User Datagram Protocol (UDP) versus Transmission Control Protocol (TCP)

Notes



Voice Packetization

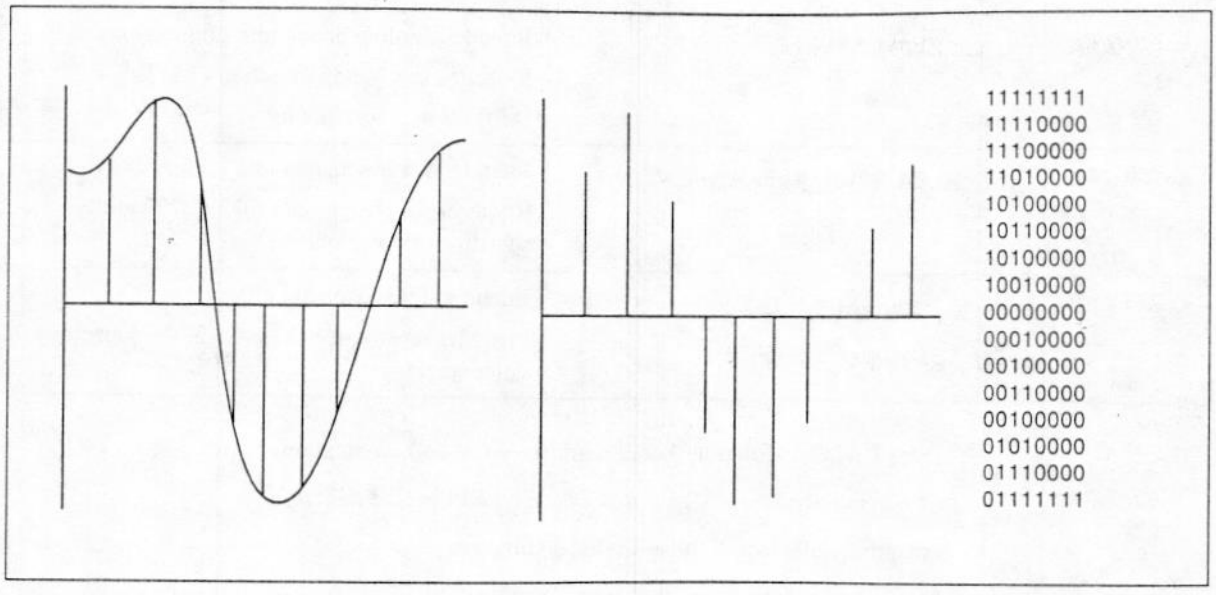
CODECs

For an analog (pulse) signal to travel across a digital network, it must first be converted into a digital (number) format. A CODEC (or coder and decoder) is a device that applies algorithms, or rules, to perform this conversion.

Sample Rate

The sample rate is the number of samples of a sound that are taken per second to represent the signal digitally. To accurately convert an analog signal into a digital signal, the sample rate must be at least twice the highest frequency of the signal. Therefore, an analog signal is sampled at a rate of 8 kHz per second, or 8000 times per second.

Figure 1: Analog-to-Digital Conversion



Notes

CODEC Selection

Selecting the appropriate speech CODEC is essential. CODEC performance includes the baseline quality (that is, without impairments) and the performance with impairments present, such as background noise and lost or late packets.

The table below shows some CODECs that are used for voice traffic. Bandwidth requirements are estimates.

Table 1: CODECs Used for Voice Traffic

CODEC	Description	Use
G.711	64 Kbps PCM[1]	Intended for high bandwidth connections Delivers optimal voice quality (toll) but requires the most bandwidth CODEC of choice when bandwidth is not an issue
G.729A/B	8 Kbps CS-ACELP[2]	Intended for low bandwidth connections Requires less bandwidth than G.711 Delivers near toll quality voice
G.726	16, 24, 32, 40 Kbps ADPCM[3]	Intended for low bandwidth connections Requires less bandwidth than G.729 at the sacrifice of voice quality
G.723.1	6.3 Kbps MPMLQ[4] 5.38 Kbps CS-ACELP[2]	Intended for low bandwidth Provides most voice channels at the sacrifice of voice quality

[1] Pulse Code Modulation (benchmark for voice communications)

[2] Conjugate Structure-Algebraic Code Excited Linear Prediction

[3] Adaptive Differential Pulse Code Modulation

[4] Multi-Pulse-Maximum Likelihood Quantization

Notes

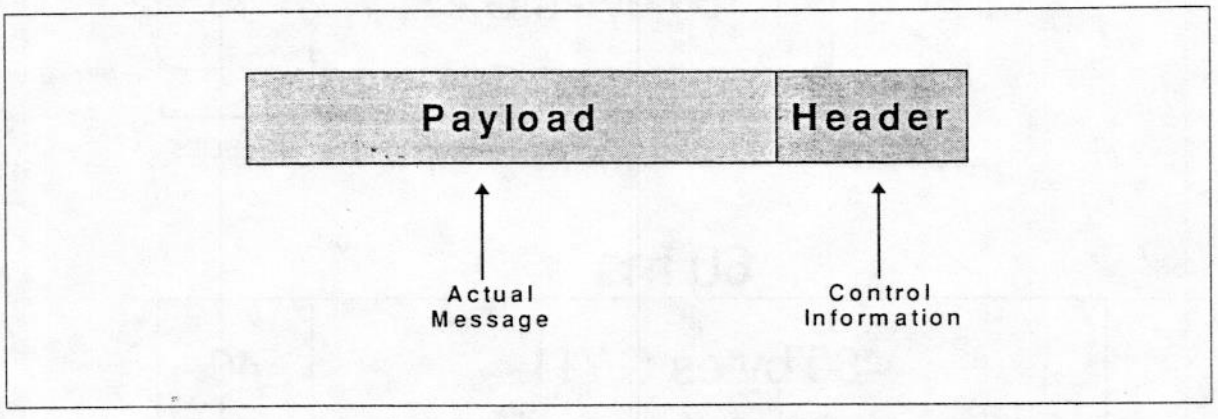
Voice Packet

The voice information is divided into packets, also known as datagrams. Each packet is transmitted individually across the packet-switched network, often following different routes to the destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

There are two main parts of the voice packet:

- **Header:** Contains control information necessary to deliver the packet
- **Payload:** Contains the actual message

Figure 2: Voice Packet

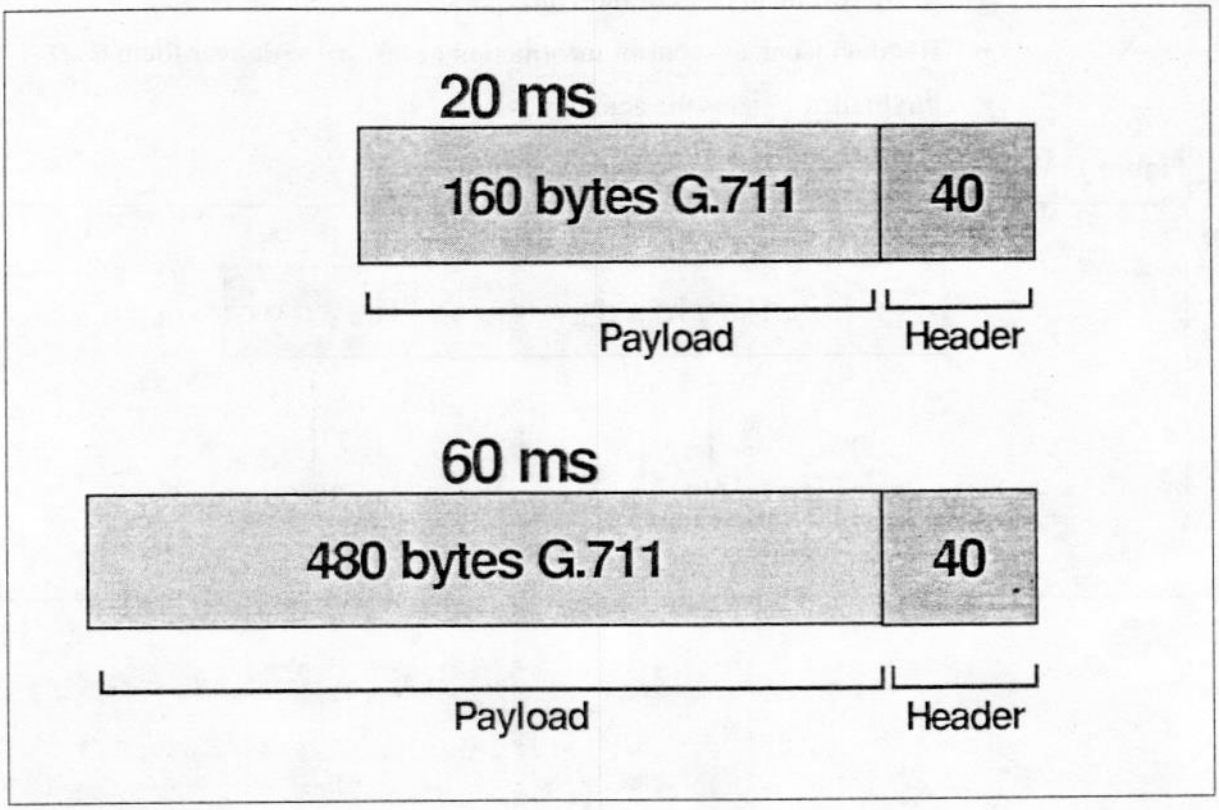


Notes

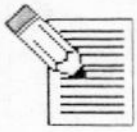
How Overhead Impacts Packet Size

Packet size is not a significant concern to traditional data (non-voice). For voice communications, however, packet size is an important consideration. As a result, for bandwidth purposes, you must factor in the bandwidth associated with the overhead.

Figure 3: How Overhead Impacts Packet Size



Notes



Comparing Packet-Switching Models

Voice over Internet Protocol (VoIP), Voice over Frame Relay (VoFR), and Voice over Asynchronous Transfer Mode (VoATM) are the three common types of packet-switching models for voice transmissions.

Because the VoIP model uses public networks, additional protocols are required to help ensure that packets get delivered in a timely manner. Some of these include User Datagram Protocol (UDP), Real-Time Protocol (RTP), and Real-Time Control Protocol (RTCP). See the section titled "Transport and Session Layer Internet Protocols," later in this lesson, for additional information.

Voice over Internet Protocol

The VoIP model transmits data over the LAN and WAN using the Internet Protocol (IP). IP is a connectionless Layer 3 Network Layer protocol, with no continuing connection between the end points.

IP does not make any assumptions of the underlying Layer 2 protocols. Underlying Layer 2 protocols can include: Ethernet, ATM, PPP, Frame Relay, and Wireless protocols.

Note: The term "Layer" refers to seven communication layers of the Open Systems Interconnection, or OSI, model, which standardizes concepts and facilitates understanding of the data communication architectures. See the "Resources" section of this guide for additional information about the OSI Model.

Voice over Internet Protocol Packet

Each VoIP packet is treated as an independent unit of data. Each computer, or host, has at least one IP address that uniquely identifies it from all other computers on the Internet. A VoIP packet contains both the sender's Internet address and the receiver's address.

Notes

Voice over Frame Relay

Frame Relay (FR) is a high-speed, packet switching Layer 2 WAN protocol. FR transmits data in variable-size units called frames over a permanent virtual circuit (PVC) that connects distant locations.

Frame Relay Frame

There are six bytes of overhead per frame. This small amount of overhead makes FR an attractive choice for communications. The address field can range from two to four bytes in length. The header can be adjusted for large networks that require additional addresses.

Voice over Asynchronous Transfer Mode

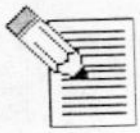
Asynchronous Transfer Mode (ATM) is a Layer 2 LAN and WAN protocol. ATM transmits data in fixed-size units called cells, which are 53 bytes in size. During the transmission, ATM creates a fixed channel, or route, between two points. This makes it easier to track and bill usage across an ATM network, but makes it less adaptable to sudden surges in network traffic.

ATM offers no guarantee of prioritization, unless the customer has purchased a Constant Bit Rate (CBR) service. The CBR provides a dedicated channel with a fixed bandwidth, based on the needs of the application.

Voice over Asynchronous Transfer Mode Cell

ATM uses a fixed-length packet, or cell, for transport. The ATM cell has a 5-byte header and a 48-byte payload (53 bytes total). ATM also has additional overhead of up to 15 percent for header information associated with VoIP transmissions. This impacts how the frame is segmented and the CODEC used. There is no trailer for this type of cell, because there is no error checking procedure. However, the header includes an error checking mechanism to ensure delivery to the correct destination.

Notes



Calculating Bandwidth for Different Compression Standards

The bandwidth required is directly related to the voice sample size and speech CODEC used. Generally, the smaller the voice sample, the greater the number of packets needed.

To calculate the approximate bandwidth for different compression standards, use the following formula:

(Bytes of Voice Payload + IP header)
x IP packets generated per second of voice
x 8 bits per byte

Table 2: Calculating Bandwidth for Different Compression Standards

CODEC	Voice Sample Size	IP Packets Generated for 1 Second of Voice	The Math	IP Bytes Required for 1 Second of Voice	Effective Bandwidth
G.711	5 ms = 40 bytes	200	(40 + 40) x 200 =	16,000	128 Kbps
G.711	10 ms = 80 bytes	100	(80 + 40) x 100 =	12,000	96 Kbps
G.711	20 ms = 160 bytes	50	(160 + 40) x 50 =	10,000	80 Kbps
G.729A/B	5 ms = 5 bytes	200	(5 + 40) x 200 =	9,000	72 Kbps
G.729A/B	10 ms = 10 bytes	100	(10 + 40) x 100 =	5,000	40 Kbps
G.729A/B	20 ms = 20 bytes	50	(20 + 40) x 50 =	3,000	24 Kbps

Notes

Transport and Session Layer Internet Protocols

Earlier you learned how the CODEC selection and type of VoIP packet-switching model impact voice transmissions. This section briefly describes some Layer 4 and Layer 5 protocols that can be used to implement VoIP performance.

Transmission Control Protocol

TCP is highly reliable and connection-oriented Layer 4 protocol. TCP provides flow control and acknowledgements of traffic, as well as the ability to retransmit data, as necessary. Because of these characteristics, TCP is best suited for situations when the integrity of the data is more important than the end-to-end transmission time. TCP is not recommended for real-time traffic because its features, and its slow start, introduce delay that can jeopardize voice QoS.

Real-Time Protocol → LAYER 5

RTP is well-suited for time-sensitive applications, such as real-time voice, fax, and video. RTP is intended as a framework, not a separate layer. Because of this, it works well with RTCP and UDP. Some major components of RTP are:

- **RTP Timeclock:** Autonomous clock source that determines how many clock ticks have occurred
- **RTP Timestamp:** Counter value that shows when the packet was created; supports silence suppression and jitter calculation
- **Synchronization Source (SSRC):** Unique, randomly generated identifier that the RTP client uses to identify the RTP session; enables you to tell which parties are talking and which parties are silent
- **Contributing sourCe (CSRC):** Identifier list following the fixed RTP packet header; preserves the identity of the original source
- **Payload Identification:** Traffic identification; for example, G.729.
- **Sequence ID:** Part of header information
- **Feedback on Jitter:** Feedback on jitter for possible adjustment to buffer

Real-Time Control Protocol

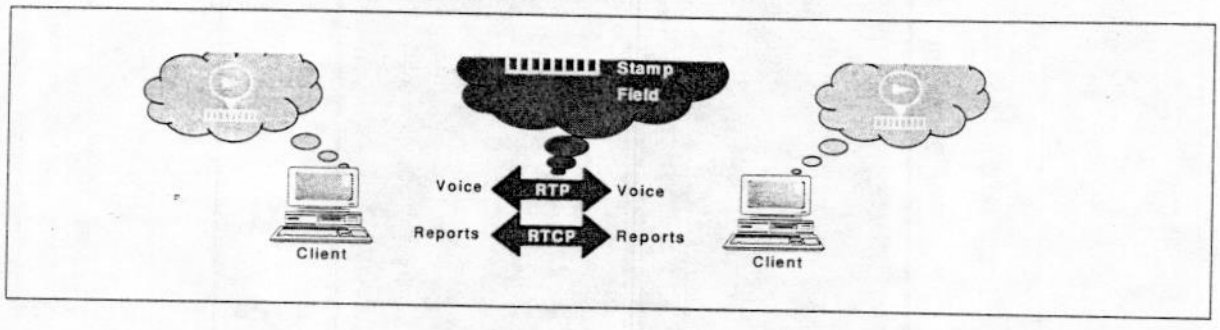
Real-Time Control Protocol (RTCP) augments RTP. RTCP is designed to monitor the quality of service and to convey information about the participants in a real-time session. Because RTP runs over UDP, neither end really knows if the RTP packets are actually delivered. RTCP solves this problem by providing feedback in the form of RTCP QoS reports to the sending party. RTCP also provides information about the sender, such as the sender's name and telephone number.

Interaction between Real-Time Protocol and Real-Time Control Protocol

RTP provides an end-to-end delivery service for real-time traffic. The figure below shows the interaction between RTP and RTCP:

- RTP carries the data that contains the real-time properties.
- RTCP monitors the QoS and generates reports about the participants in the ongoing session

Figure 4: Interaction between RTP and RTCP



User Datagram Protocol

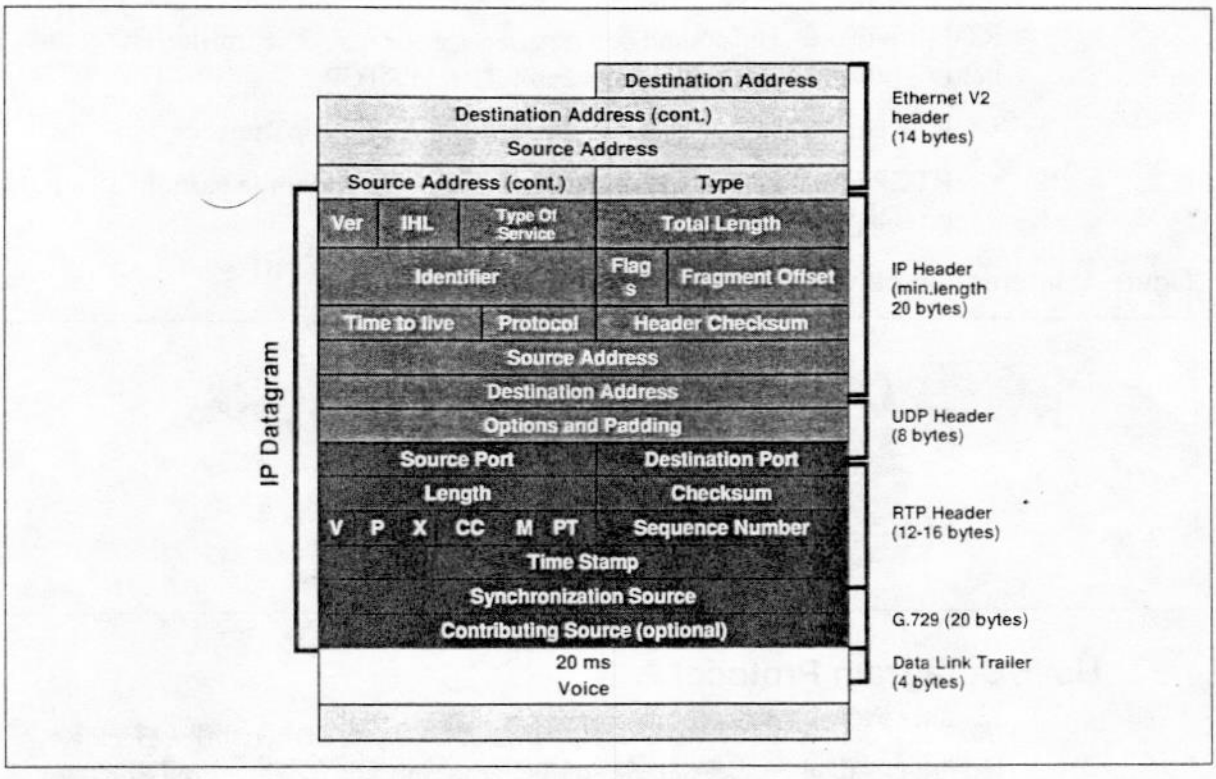
UDP is a connectionless protocol that runs on top of IP networks. Because UDP lacks many of the features of TCP that introduce delay, such as flow control and error recovery, UDP is well-suited to voice traffic.

Notes

Relationship between User Datagram Protocol Packet and Real-Time Protocol Header

The UDP packet does not supply sequence numbers, timestamps, audio source identification, CODEC type, and other information important to the delivery of real-time information. Because of this, another header, such as the RTP header, is required to supply the missing information. The figure below shows how the UDP packet and RTP header work together.

Figure 5: User Datagram Protocol Packet and Real-Time Protocol Header



Notes

Major Components of Voice over Internet Protocol

To deploy VoIP, it is necessary to add hardware to support both VoIP communications and the new product offerings introduced with VoIP, such as open (as opposed to proprietary) IP terminals and unified messaging (voice, fax, data, multimedia).

Some major components that comprise the VoIP model are:

- **Call Servers:** Provide call processing for client devices, as well as proxy interworking with intelligent terminals and devices
- **Call Signaling Servers:** Include an industry-standard Central Processing Unit (CPU) to drive the signaling for IP terminals and other IP devices
- **H.323 Gateways:** Provide access to Public Switched Telephony Networks (PSTNs) and analog devices through a locally routed, direct IP media path
- **Media Gateways:** Increase the system capacity to support additional trunks, analog and digital telephones, and IP terminals
- **Gatekeepers:** Provide address translation, admissions control, and bandwidth control
- **IP Terminals and Clients:** Connect directly to the LAN through the Ethernet connection to bring voice and data communications to the end user; an IP telephony server completes the call processing
- **IP Network:** Provides the universal communication language and foundation to allow dissimilar networks and equipment from a variety of vendors to interconnect

Detailed information about the technologies and protocols that drive these devices is located in the "Voice over Internet Protocol Standardization and Signaling Protocols" lesson, later in this course.

Note: H.323 is a packet-based signaling standard that provides a foundation for audio, video, and data communications across IP-based networks, including the Internet.

Notes

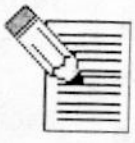
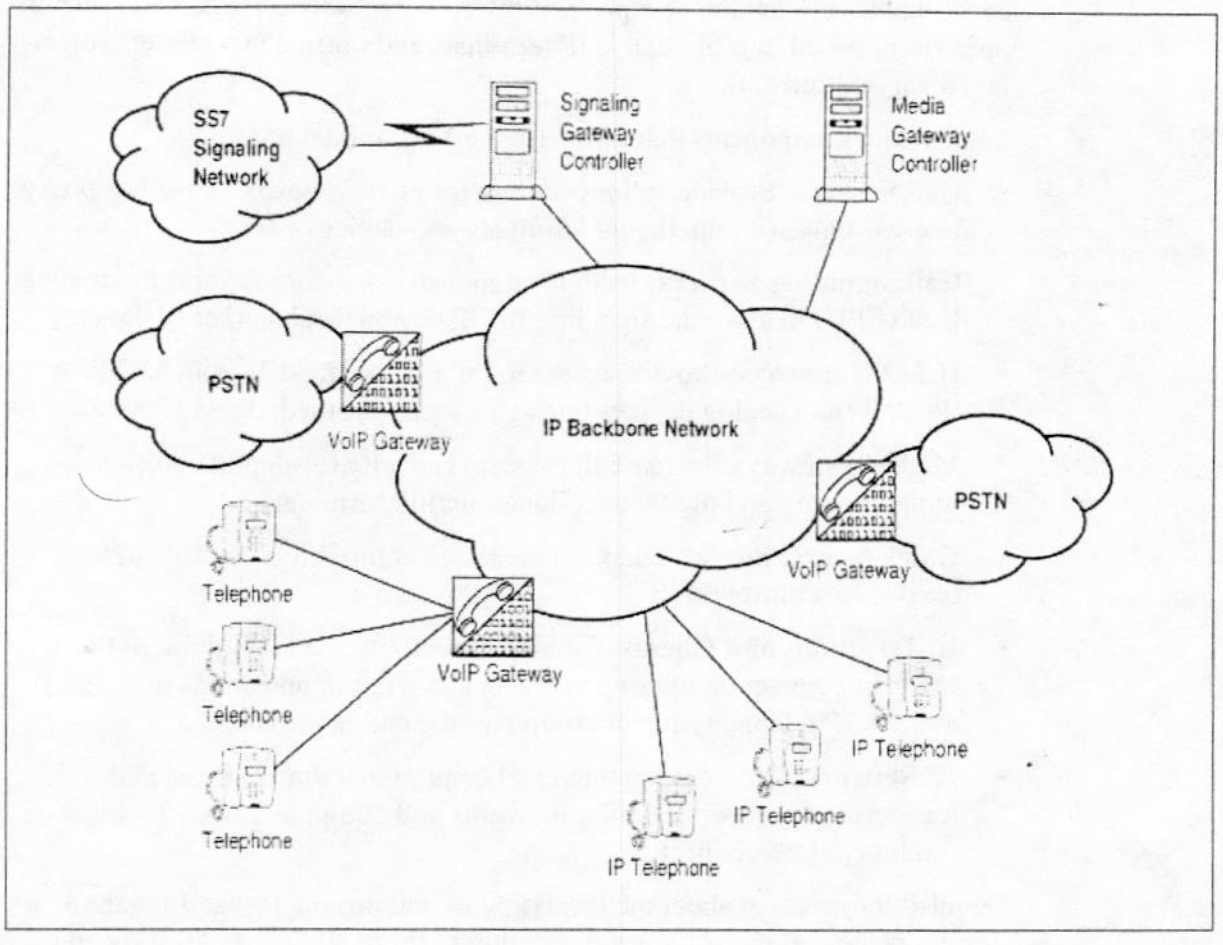
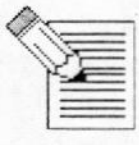


Figure 6: Major Components of Voice over Internet Protocol



Notes



Practice

Answer the following questions.

1. A customer requires the least amount of bandwidth usage and is not concerned with voice quality. Which CODEC would you recommend?

   a. G.711
   b. G.729A
   c. G.723.1
   d. G.726

2. A customer requires the best balance of quality audio and bandwidth savings. Which CODEC would you recommend?

   a. G.711
   b. G.729A
   c. G.723.1
   d. G.727

3. At what rate is an analog signal sampled using a G.711 CODEC?

   a. 2 kHz
   b. 3 kHz
   c. 4 kHz
   d. 8 kHz

Notes

4. What are the two main parts of a voice packet?

   a. Header and Payload
   b. Leader and Header
   c. Footer and Load
   d. Leader and Message

5. On which layer of the OSI model does IP reside?

   a. Layer 1
   b. Layer 2
   c. Layer 3
   d. Layer 5

6. Which Layer 2 protocol transmits data at a fixed size unit called a cell?

   a. PPP
   b. ATM
   c. PPTP
   d. CBR

7. Given the following parameters:

   - G.711 CODEC
   - 10 ms Voice sample
   - IP packet header is 40 bytes

   Ignoring Layer 2 information, what is the expected bandwidth required per call?

   a. 256 kbps
   b. 128 kbps
   c. 96 kbps
   d. 80 kbps

8. Given the following parameters:

   - G.729 CODEC
   - 20 ms Voice sample
   - IP packet header is 40 bytes

   Ignoring Layer 2 information, what is the expected bandwidth required per call?

   a. 96 kbps
   b. 72 kbps
   c. 48 kbps
   d. 24 kbps

9. Which Protocol is highly reliable, connection oriented and best suited for situations when the integrity of the data is more important than the end-to-end transmission time?

   a. UDP
   b. TCP
   c. RTP
   d. PPP

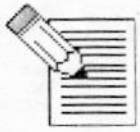
10. Which protocol is designed to monitor the Quality of Service and to convey information about participants in a real-time session?

    a. RTCP
    b. IP
    c. TCP
    d. SIP

Answers to Practice

If you successfully completed the Practice and are confident with your understanding of the material, you have satisfied the lesson requirements.

Notes



Summary

In this lesson, you reviewed general information about packet telephony, such as voice sampling and bandwidth calculations, based upon different compression standards. You learned about basic differences in packet-switching models, such as VoIP, VoFR, and VoATM. You also learned how attributes of RTP and UDP make these protocols ideal to meet the needs of real-time applications.

Notes

Notes

Packet Telephony Design Issues

Introduction

This lesson builds upon basic concepts covered in the previous lesson, such as: voice packetization, overhead, payload, bandwidth, compression, protocols, and types of packet-switched networks.

In this lesson, you will learn packet design techniques to help ensure that the voice quality on the data network meets the customer's expectations.

Objectives

Given this module and the instructor's presentation, you will be able to complete these tasks:

- Apply knowledge of latency and packet loss to select CODECs that meet the customer's voice quality expectations
- Determine bandwidth requirements based upon call volume and voice packetization parameters
- Apply knowledge of the voice quality tests to express the level of voice quality

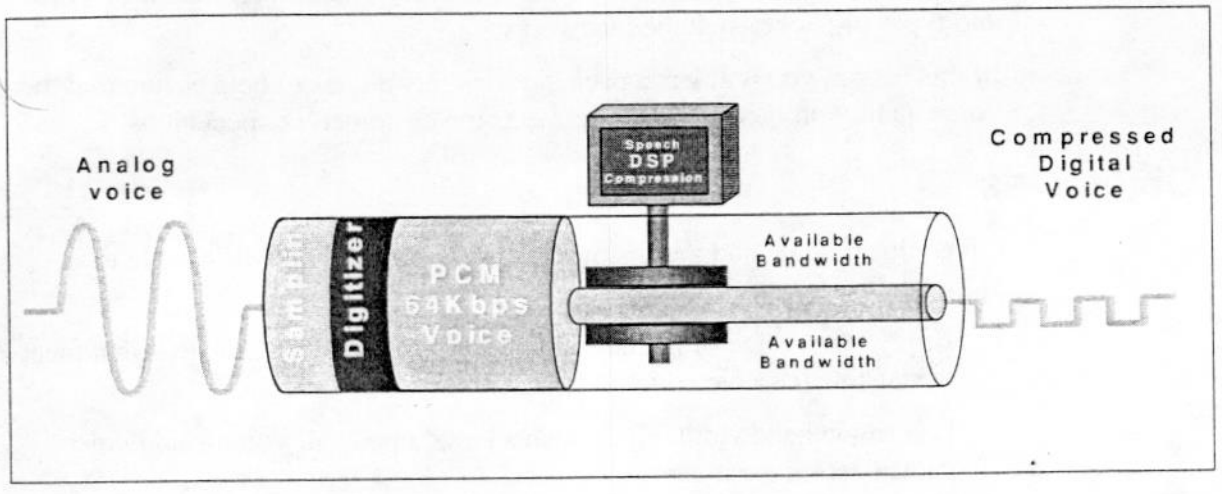
Notes

Voice Quality on a Data Network

Performance of Speech CODECs Based Upon Compression Standards

Speech CODECs (compression algorithms), such as G.729 and G.723, are intended to reduce the bandwidth required. The key is to select a CODEC that meets both the bandwidth and voice quality requirements.

Figure 1: Speech Compression



Voice Quality Measurement

Two models that measure voice quality are:

- Mean Opinion Score (MOS)
- E-Model G.107

Both models are covered in greater detail, later in the lesson.

Notes

Voice Quality Versus Bandwidth Reduction

The trade-offs for reducing bandwidth are:

- End-to-end delay (latency)
- Distortion in voice quality

The table below shows that the result of increased voice compression is increased delay and lower voice quality.

Table 1: Performance of Speech CODECs Based Upon Compression Standards

CODEC	Sample Time	Look Ahead Delay	Minimum Compression Algorithm Delay	Voice Quality
G.711 (64 Kbps)	.125 ms	Not applicable	.125 ms	Toll quality
G.729 (8 Kbps)	10 ms	5 ms	15 ms	Near toll quality
G.723 (5.38/6.3 Kbps)	30 ms	7.5 ms	37.5 ms	Fair to good

Note: Although there are many CODECs from which you can select, the CODECs used most often are G.711 and G.729. Values listed in the table are estimates.

Notes

All Networks Experience Delay

Although some CODECs have a higher compression algorithm delay (encoding and decoding time), all networks experience some delay.

Packet delay has a significant impact on the perceived quality of a voice. To improve overall Quality of Service (QoS), it is vital to detect the delay and compensate for it. Techniques, such as queueing and prioritization, can significantly improve overall network performance and voice quality.

You will learn more about QoS mechanisms in the next lesson.

Tip: *Delay should be less than 150 to 200 ms to avoid complaints, depending upon the types of applications used and customer requirements.*

Two Types of Delay

There are two types of delay:

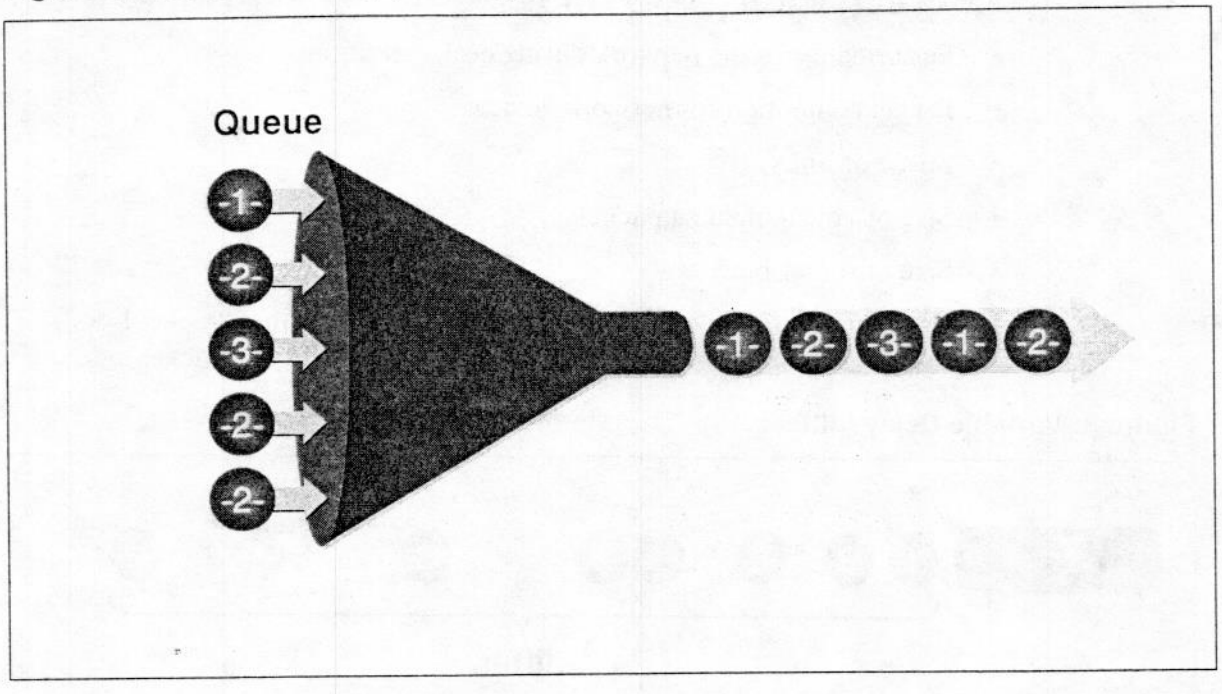
- End-to-end delay (latency)
- Variable delay (jitter)

Notes

End-to-End Delay (Latency)

End-to-end delay (latency) is a non-variable (fixed) value. It is the time between the generation of a sound at one end and the reception of the sound at the other end.

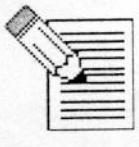
Figure 2: End-to-End Delay (Latency)



Some factors that influence end-to-end delay are:

- **Processing:** Time needed to encode, packetize, and decode the transmission
- **Propagation:** Distance between source and destination
- **Data network transmission:** Link speed (per network segment)

Notes



Variable Delay (Jitter)

Variable Delay (jitter) is dynamic. Jitter produces gaps in the conversation due to an uneven flow of data.

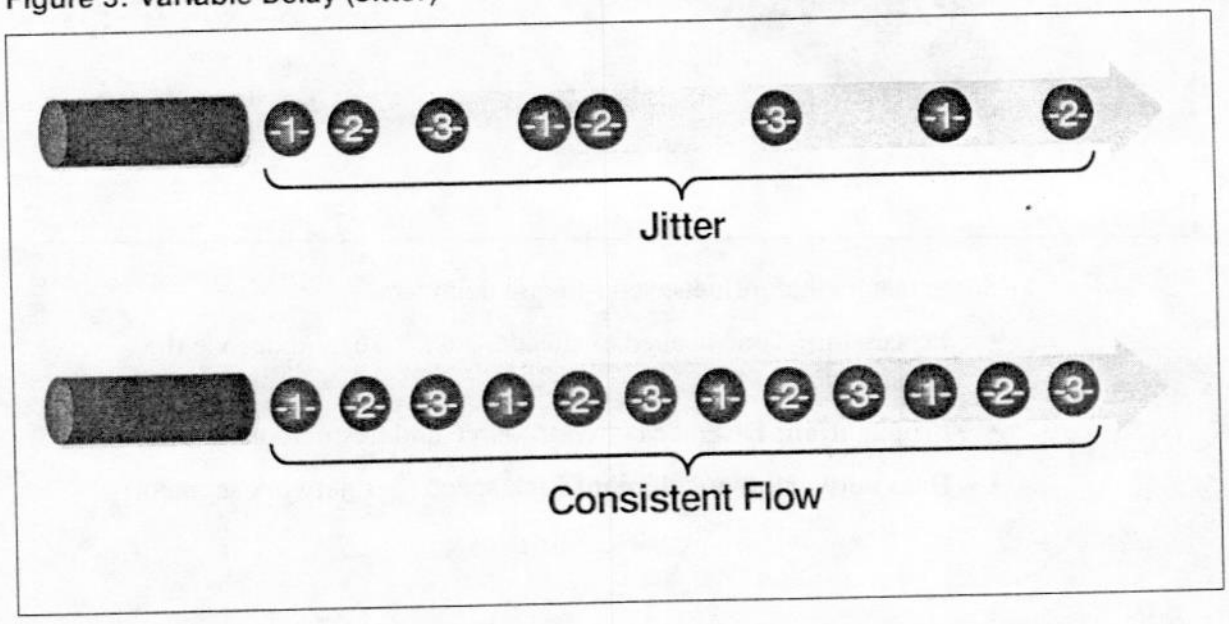
Factors that Impact Variable Delay (Jitter)

Some factors that contribute to jitter are:

- Performance of the network during peak conditions
- Packet contention for network devices
- Speed of links
- Size of voice and data packets
- Size of router buffers

However, uncontrollable jitter impacts packet loss. See the "Packet Loss" section, later in this lesson, for additional information about packet loss.

Figure 3: Variable Delay (Jitter)



Notes

Techniques to Compensate for Delay

Some techniques to compensate for delay are:

- **Differentiated Services (DiffServ):** Allows you to define different service classes and QoS mechanisms for packets (Layer 3)
- **Resource ReSerVation Protocol (RSVP):** Allows the receivers to reserve a dedicated portion of the network's bandwidth
- **Ethernet 802 Standards:** Provide congestion management at LAN port and user levels (802.1p and 802.1Q)
- **Port-based Prioritization:** Allows you to configure a Layer 2 switch to prioritize all traffic originating from a specific port; for example, a VoIP gateway
- **Traffic Separation:** Allows you to separate voice and data traffic via a virtual LAN (VLAN)
- **IP Address Prioritization:** Allows you to prioritize all packets originating from designated IP addresses

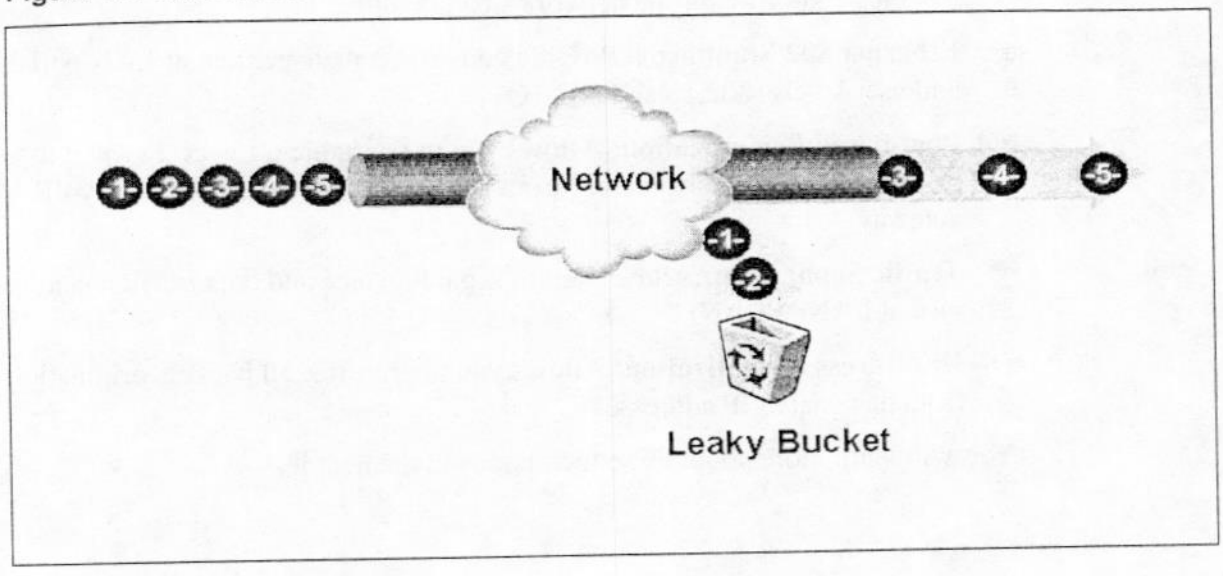
You will learn more about these techniques in the next lesson.

Notes

Packet Loss

Sometimes packets fail to arrive at the destination. This creates gaps in conversation that degrade the voice quality; for example, clicks, muting, or unintelligible speech.

Figure 4: Packet Loss



Tip: *Keep packet loss below one percent.*

Notes

Factors that Impact Packet Loss

Some factors that impact packet loss are:

- **Congestion:** Router discards packets to reduce congestion, or the buffer overflows
- **Service Disruption:** Network experiences an outage
- **Delay:** Some packets take a longer route or experience delays that prevent them from reaching their destination at the appropriate time
- **CODEC Selection:** Coding and decoding delay; for example, G.723 has a higher algorithmic delay than G.711, which can impact voice quality

Caution: *Packet loss will vary, depending upon the compression method (CODEC) used. Higher compression ratios increase the susceptibility of voice quality to packet loss.*

Techniques to Control Packet Loss

Ways to avoid packet loss include:

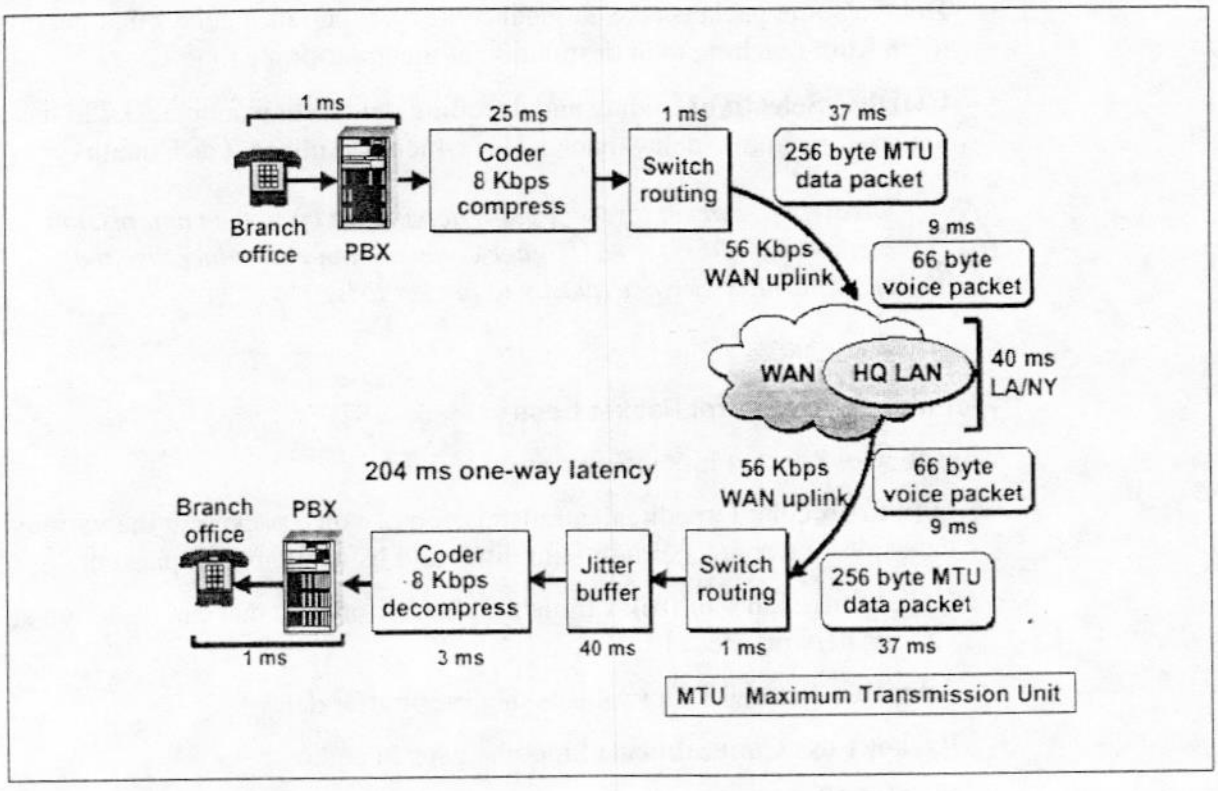
- **QoS Protocols:** Expedite the transmission of voice packets at the various gateways and routers, minimizing jitter and its resultant lost packets
- **Call Admission Control:** Limits the number of calls that can be active at various network nodes
- **Adaptive Jitter Buffer:** Adjusts the jitter buffer delay
- **Packet Loss Concealment:** Smooths gaps in audio
- **Bandwidth Increase:** Increases bandwidth to handle peak traffic loads; compensates for packet loss that is often concealed by the retransmissions of data protocols

Notes

Example: Delay

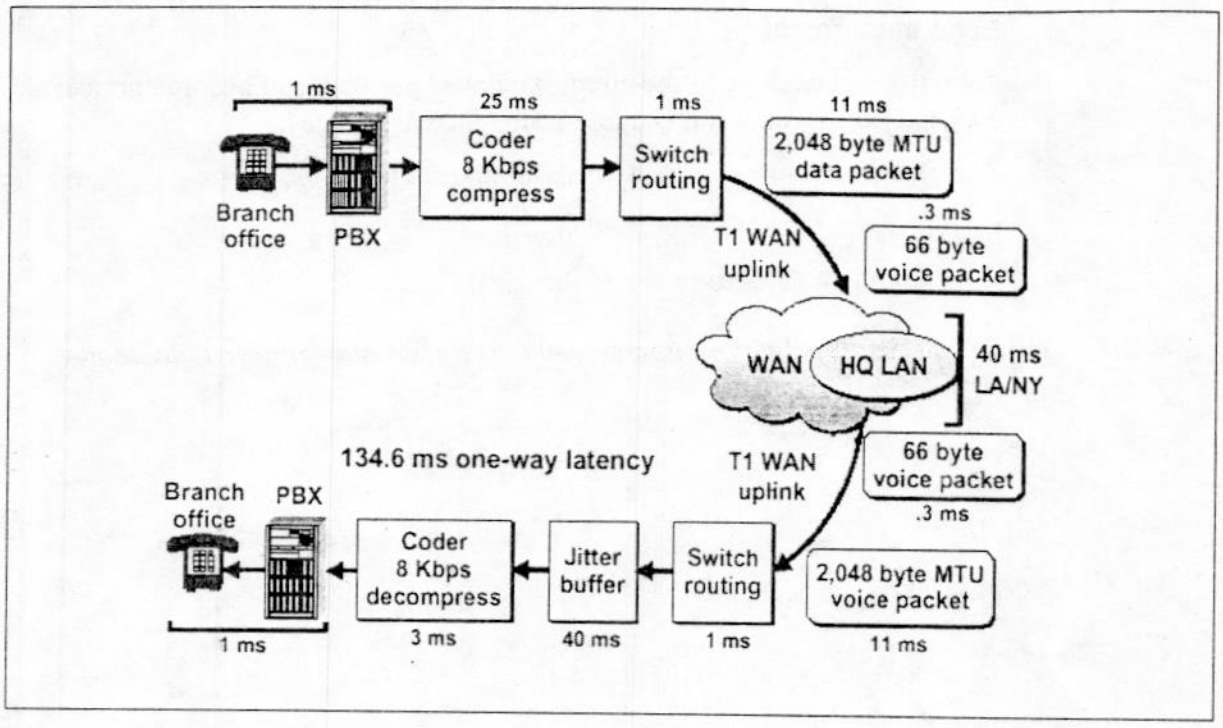
The figure below provides an example of the delays that a voice packet experiences as the packet moves through the WAN. Contrast this example with the figure on the next page that uses T1 links.

Figure 5: Estimated Latency: 56 Kbps WAN Links



Notes

Figure 6: Estimated Latency: T1 WAN Links



Notes

Echo Impairment and Control

Echo Impairment

Echo that is inaudible in the circuit-switched network can become noticeable with packet transmission because of the increased delay.

Two factors that impact the severity of an echo are:

- The amplitude of the echoed signal
- The time it takes to return to the speaker

Tip: *It is important to detect and remove echo greater than 28 ms.*

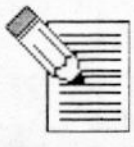
Notes

Devices to Control Echo

Devices that control echo are:

- **Echo Canceller:** An echo canceller is a device that looks for echo (a delay on the return path that is strongly correlated with a signal seen on the incoming path) and uses an adaptive filter to model the echo and then subtract it from the return signal. An echo canceller can improve the echo path loss of a connection by up to 26 to 30 dB with the adaptive filter. Any residual echo is removed using a non-linear processor, which removes all signals below a certain threshold.
- **Echo Suppressor:** An echo suppressor, or voice switch, is a device that detects a signal on the incoming or outgoing path and switches attenuation into the other path to reduce the level of any returning signal. This suppression technique can be used in speakerphones, headsets, and wireless handsets.

Notes



Calculating Bandwidth

In the previous lesson, you learned how CODEC selection impacts the packet overhead. Another important factor is the data link layer network technology that is used.

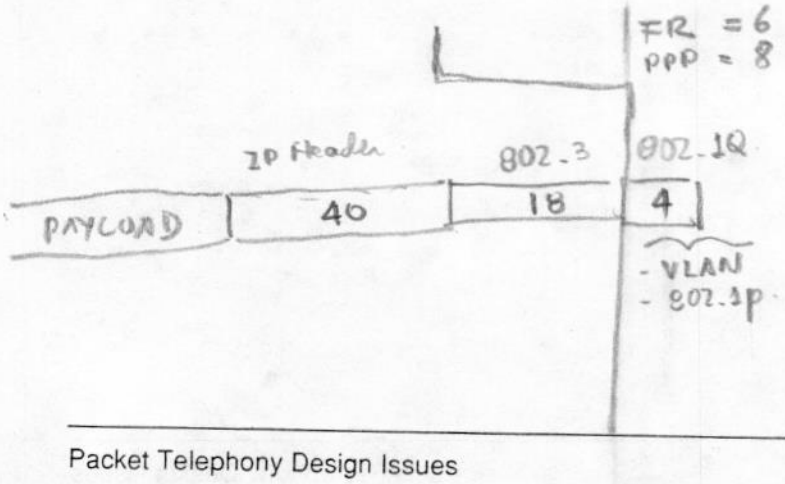
For example, assuming a 40-byte base IP header:

- If you are using a Point-to-Point Protocol link, add 8 bytes to the base header size, for a total header size of **48 bytes**.
- If you are using a Frame Relay link, add 6 bytes to the base header size, for a total header size of **46 bytes**. (If you are using longer Frame Relay addresses, this value will be higher.)
- If you are using Ethernet (802.3), add 18 bytes to the base header size, for a total header size of **58 bytes**. (If you are using 802.1Q tagging, this value will be higher.)

See the table below for details. See the next page for the calculations.

Figure 7: How Link Layers Impact Overhead

Codec	Sample (ms)	IP Header (IP/UDP/ RTP)	802.3	Frame Relay	PPP	ATM (IP/AAL-5)	ATM (AAL-5)
G.711	10	40	18	6	8	39	26
G.711	20	40	18	6	8	65	52
G.711	30	40	18	6	8	38	78
G.711	40	40	18	6	8	64	51
G.711	60	40	18	6	8	63	103
G.729 A/B	10	40	18	6	8	56	43
G.729 A/B	20	40	18	6	8	46	33
G.729 A/B	30	40	18	6	8	36	23
G.729 A/B	40	40	18	6	8	26	13
G.729 A/B	60	40	18	6	8	59	46



Example 1:

- CODEC G.711 = 64 Kbps
- Voice payload (sample) = 10 ms (80 bytes)
- IP header = 40 bytes
- Link type = 802.3 (Ethernet) 18 bytes
- IP packets per second = 100

The math: (80 + 58) x 8 x 100 = 110,400 (110.4 Kbps)

Example 2:

- CODEC G.729 = 8 Kbps
- Voice payload (sample) = 10 ms (10 bytes)
- IP header = 40 bytes
- Link type = PPP 8 bytes
- IP packets per second = 100

The math: (10 + 48) x 8 x 100 = 46,400 (46.4 Kbps)

Notes

Knowledge Check

The following figure shows bandwidth requirements per call and maximum number of voice calls depending on voice CODEC, voice payload and link speed for Ethernet, Frame Relay and Asynchronous Transfer Mode (ATM) networks. Use the figure below to answer the questions that begin on the next page.

Important: The table assumes an 85 percent theoretical throughput.

	G.711			G.729		
Codec Bit Rate	64kbps			8kbps		
Voice Sample (ms)	10	20	30	10	20	30
IP Payload size (bytes)	80	160	240	10	20	30
IP Packet size (40 byte header)	120	200	280	50	60	70
Ethernet						
Ethernet bytes (per packet)	150	230	310	80	90	100
Ethernet bandwidth per voice flow (kbps)	130	96.8	85.9	73.6	40.8	29.9
Number of Voice Calls, Assuming 50% Link Utilization for Voice Traffic						
10 Mbps	38	51	58	67	122	167
100Mbps	385	516	582	679	1225	1674
1 Gbps	3858	5165	5823	6793	12254	16742
Frame Relay						
Frame Relay bytes (per packet)	124	204	284	54	64	74
Frame Relay bandwidth per voice flow (kbps)	100	82.0	76.0	44.0	26.0	20.0
Number of Voice Calls, Assuming 50% Link Utilization for Voice Traffic						
64 kbps	0	0	0	0	1	1
128kbps	0	0	0	1	2	3
384 kbps	1	2	2	4	7	9
512 kbps	2	3	3	5	9	12
1.54Mbps	7	9	10	17	29	38
2.048 Mbps	10	12	13	23	39	51
45Mbps	225	274	296	511	865	1125
ATM						
ATM cells required	3	5	6	2	2	2
ATM payload in bytes (per packet)	120	200	280	50	60	70
ATM bandwidth per voice flow (kbps)	127.2	106.0	84.8	84.8	42.4	28.3
Number of Voice Calls, Assuming 50% Link Utilization for Voice Traffic						
1.54Mbps	6	7	9	9	18	27
2.048 Mbps	8	9	12	12	24	36
45Mbps	176	212	265	265	530	796
155Mbps	609	731	914	914	1827	2742

Questions:

1. Given the following parameters:

   - CODEC is G.729
   - Voice packet payload is 10 ms
   - 1.544 Mbps Frame Relay link

   Assuming 50 percent link utilization, how many simultaneous calls can be made over the link?

   a. 7
   b. 17
   c. 27
   d. 37

2. Given the following parameters:

   - CODEC is G.711
   - Voice packet payload is 20 ms
   - 100 Mbps Ethernet link

   Assuming 50 percent link utilization, how many simultaneous calls can be made over the link?

   a. 225
   b. 316
   c. 425
   d. 516

3. Given the following parameters:

   a. CODEC is G.711
   b. Voice packet payload is 30 ms
   c. 128 kbps Frame Relay link

   Assuming 50 percent link utilization, how many simultaneous calls can be made over the link?

   a. 0
   b. 5
   c. 10
   d. 15

4. The customer needs the ability to make 385 simultaneous calls on their Ethernet network with 50 percent link utilization for voice calls. The customer wants to ensure maximum voice quality. Based upon this request, what are your recommendations to the customer about the minimum requirements to meet this need?

   a. G.729 CODEC
      20 ms Voice Sample
      10 Mbps Ethernet link

   b. G.711 CODEC
      30 ms Voice Sample
      10 Mbps Ethernet link

   c. G.711 CODEC
      10 ms Voice Sample
      100 Mbps Ethernet link

   d. G.729 CODEC
      20 ms Voice Sample
      1 Gbps Ethernet link

Common Models for Voice Quality

Once the voice quality and delay budget profiles have been outlined, it is important to monitor the voice quality of the VoIP network. Two common models used to measure voice quality are:

- Mean Opinion Score (ITU P.800)
- E-Model (ITU G.107)

Mean Opinion Score

Mean Opinion Score (ITU P.800)

The Mean Opinion Score (MOS) is a subjective rating used to rank voice quality. It uses these benchmarks:

- 5 = Person-to-Person (excellent)
- 4 = Phone quality (good)
- 3 = Adequately understandable, but not very good quality (fair)
- 2 = Can understand words, but cannot recognize speaker (poor)
- 1 = Cannot understand words or recognize the speaker (bad)

An MOS of 4.0 is considered good. An MOS of 3.6 or less is considered poor.

The MOS is generally used with circuit-switched environments. For VoIP, the E-Model is recommended. See the next section for details.

Notes

E-Model

The E-Model is a transmission-planning tool for estimating the user satisfaction of a narrowband (300 to 3400 Hz) handset conversation, as perceived by the listener. It is defined in ITU G.107. The E-Model is well-suited for VoIP. The output of the E-Model is the Rating Factor, the R-Value, or simply R.

The scale is typically from 50 to 94, where everything below 50 is clearly unacceptable and everything above 94.15 (the maximum with the G.107 E-Model version 19 default values at 0 ms) is unobtainable in narrowband telephony.

R is calculated from a number of parameters, such as loudness, echo, and delay, but it takes into account the effects of packet loss and speech compression codecs with the equipment impairment factor.

The basic equation for the model is:

$$R = Ro - Is - Id - Ie + A$$

Where:

- **Ro** = Base R-Value, such as noise
- **Is** = Impairments that are simultaneous to speech, such as echo
- **Id** = Impairments that are delayed after speech
- **Ie** = Impairments due to the effects of special equipment, such as codecs
- **A** = Advantage factor (to take account of user advantages, such as mobility)

Notes

R-Value

The R-Value is calculated on a value called the Impairment Factor. The Impairment Factor is based on parameters, such as: loudness, echo, delay,

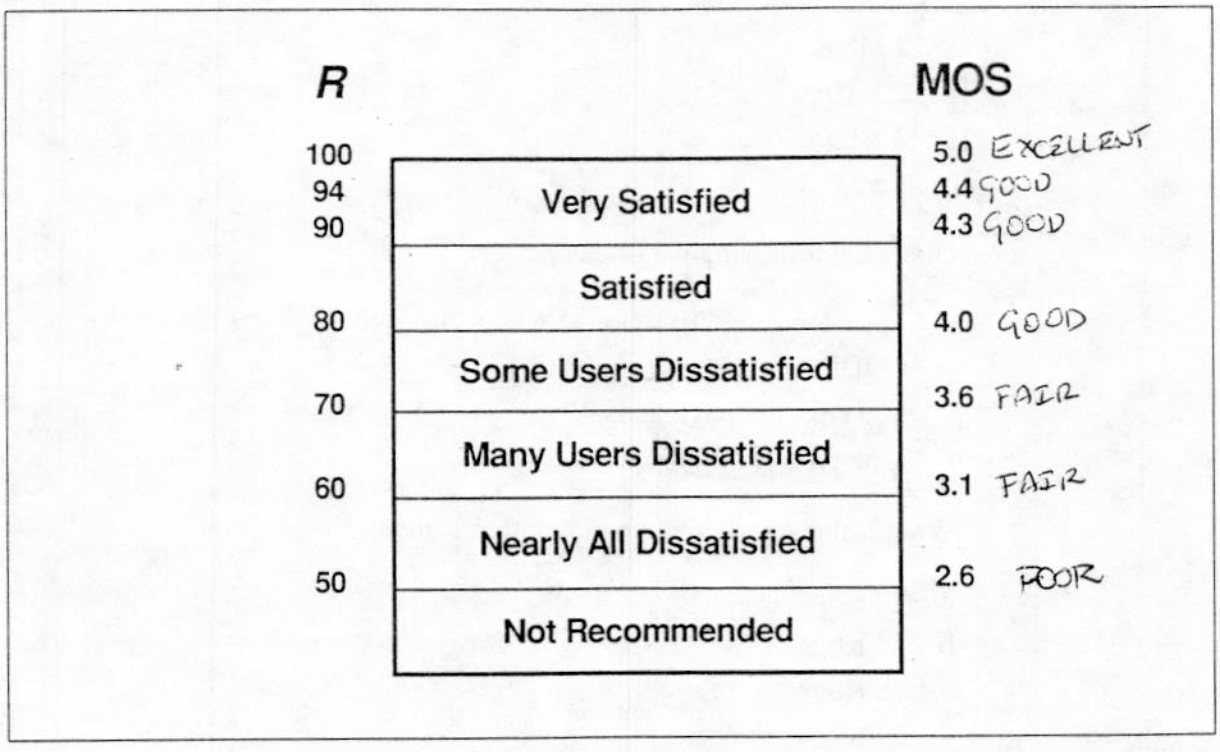
Recommended Minimum R-Value

The recommended minimum R-Value is 70. An R-Value under 50 is considered unacceptable. An R-Value greater than 94.5 is considered unobtainable in narrowband telephony.

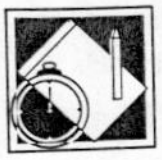
R-Value Mapped to MOS

Once an R-Value is obtained, it can be mapped to an estimated MOS, as shown in the below figure.

Figure 8: R-Value Mapped to MOS



Notes



Practice

Answer the following questions.

1. Given the following parameters:

   - Voice Activity Detection (VAD) is disabled
   - CODEC is G.711
   - Voice packet payload is 20 ms
   - 40 simultaneous calls

   What is the approximate bandwidth required for running on an Ethernet LAN network?

   a. 2 Mbps
   b. 2.5 Mbps
   c. 3 Mbps
   d. 3.5 Mbps

2. Given the following parameters:

   - Voice Activity Detection (VAD) is disabled
   - CODEC is G.729
   - Voice packet payload is 40 ms
   - Link type is PPP

   What is the approximate bandwidth required?

   a. 10 Kbps
   b. 14 Kbps
   c. 18 Kbps
   d. 22 Kbps

3. Given the following parameters:

   - Voice Activity Detection (VAD) is disabled
   - CODEC is G.729
   - Voice packet payload is 60 ms
   - 1.544 Mbps Frame Relay link

   Assuming 60 percent link utilization, how many simultaneous calls can be made over the link?

   a. 55
   b. 65
   c. 110
   d. 130

4. Given the following parameters:

   - Voice Activity Detection (VAD) is disabled
   - CODEC is G.711
   - Voice packet payload is 30 ms
   - 100 Mbps Ethernet switched LAN

   Approximately how many IP phones can make simultaneous calls if Call Admission Control (CAC) limits VoIP bandwidth to 20 Mbps?

   a. 250
   b. 275
   c. 300
   d. 325

5. Which non-variable value is the time between the generation of sound at one end and the reception of the sound at the other end?

   a. Jitter
   b. Buffer
   c. End-to-End Delay (Latency)
   d. Endtime

6. Which variable value is dynamic and affects the total time between the generation of sound at one end and the reception of the sound at the other end?

   a. Variable Delay (Jitter)
   b. Buffer
   c. End-to-End packet
   d. Endtime

7. What mechanism allows you to define different service classes and QoS mechanisms for packets?

   a. RSVP
   b. DiffServ
   c. VLAN
   d. Port Prioritization

8. A customer needs toll quality for their VoIP network. What MOS is considered toll quality?

   a. 1
   b. 2
   c. 3
   d. 4

9. Using the E-Model, what R-value is the recommended minimum?

   a. 70
   b. 60
   c. 50
   d. 40

Answers to Practice

If you successfully completed the Practice and are confident with your understanding of the material, you have satisfied the lesson requirements.

Summary

In this lesson, you learned about factors that impact QoS, such as:

- CODEC selection
- Delay
- Echo
- Bandwidth

You also learned about techniques to ensure that the voice quality on the data network meets the customer's expectations, including models to measure the voice quality on a network.

Notes

Traffic Convergence Issues

Introduction

Most data networks are structured to treat all traffic the same. The traffic can experience different amounts of delay and packet loss at any given time. Because of this structure, data networks are referred to as best-effort networks. This can result in poor voice quality. In contrast, voice networks are structured so that voice traffic experiences a fixed amount of delay and essentially no packet loss. This results in very high quality voice.

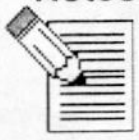
This lesson identifies some key issues that you may encounter with the deployment of a Voice over Internet Protocol (VoIP) solution over a Local Area Network (LAN) and Wide Area Network (WAN). It also describes techniques you can use to achieve End-to-End Quality of Service (QoS).

Objectives

Given the student guide and the instructor's presentation, you will be able to:

- Discriminate between the various methods available for implementing QoS prioritization of VoIP traffic to achieve the best voice quality
- Explain the issues and challenges of running VoIP over low speed WAN connections
- Define the key infrastructure needed to support the addition of VoIP traffic in the LAN and WAN environments
- Identify common Ethernet network issues known to be problematic for VoIP traffic in a LAN environment

Notes



What is Quality of Service?

There are many perceptions regarding QoS. Some of the more common views of QoS follow:

- QoS is the perception of overall voice quality by the user
- QoS is dependent on the characteristics of the IP network
- QoS is governed by the differences between cost and quality
- QoS delivers availability, reliability, and predictability
- QoS has the ability to prioritize traffic flows
- QoS manages customer's expectations through Service Level Agreements (SLAs)

Factors that Impact Quality of Service

QoS involves a broad range of technologies, architecture, and protocols. Network operators achieve end-to-end QoS by ensuring that network elements apply consistent treatment to traffic flows across the network.

However, QoS for VoIP largely depends on these network parameters:

- Jitter
- Delay
- Packet loss

Notes

> costo > BW > calidad de servicio

Trabajamos en Layer 3

Methods to Achieve Quality of Service

QoS is an architecture that delivers availability, reliability, and predictability for prioritizing traffic flows. Service Providers can use QoS to provide Service SLAs to customers and help manage their expectations. Network operators achieve end-to-end QoS by ensuring that network elements apply consistent treatment to traffic flows as they traverse the network.

Some methods to achieve quality of service for VoIP traffic are:

- **Resource ReSerVation Protocol (RSVP):** Allows the receivers to reserve a dedicated portion of the network's bandwidth
- **Differentiated Services (DiffServ):** Allows you to define different service classes and QoS mechanisms for packets
- **Ethernet 802 Standards:** Provide congestion management at LAN port and user levels
- **Port-based Prioritization:** Allows you to configure a Layer 2 switch to prioritize all traffic originating from a specific port; for example, a VoIP gateway
- **Traffic Separation:** Allows you to separate voice and data traffic via a virtual LAN (VLAN)
- **IP Address Prioritization:** Allows you to prioritize all packets originating from designated IP addresses
- **Packet Fragmentation:** Allows you to fragment packets prior to traversing bandwidth-limited connections

Note: When implementing QoS, also consider routing protocols. Routing protocols can be very important when considering how VoIP calls will be routed and how quickly fail-over occurs. When planning deployment of VoIP, the network designer must be aware of what types of situations trigger a routing table update with respect to the routing protocol. This helps predict what path VoIP traffic can take when a network failure occurs.

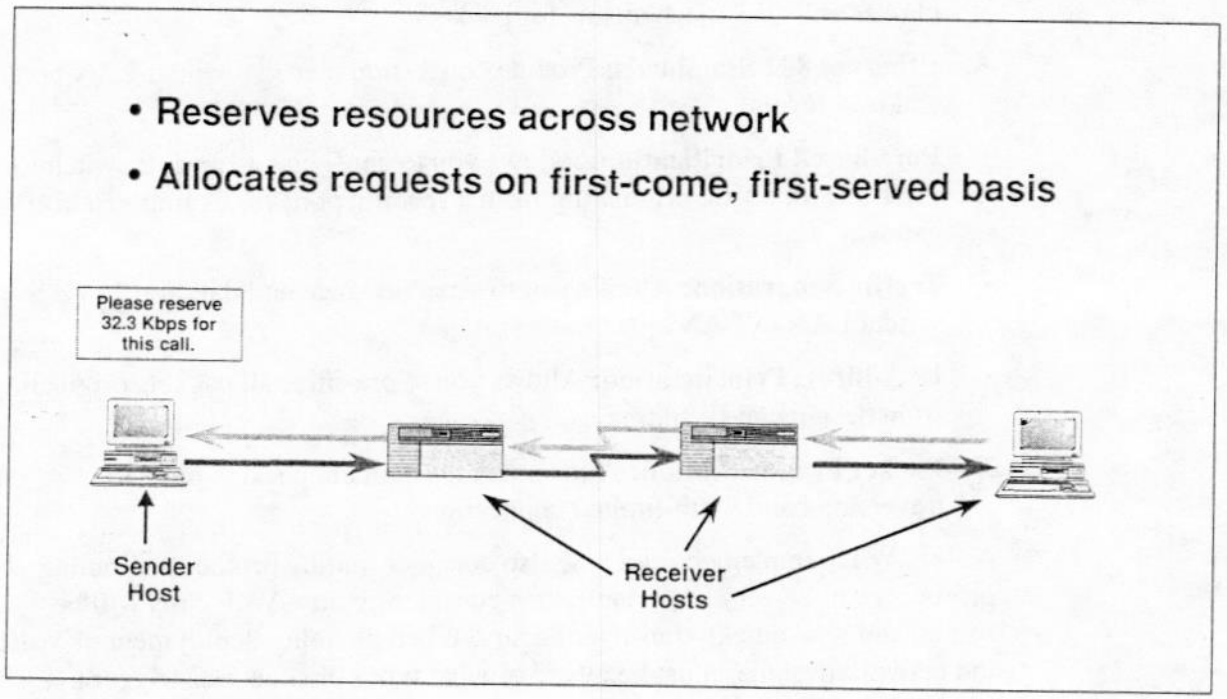
Notes

Resource ReSerVation Protocol

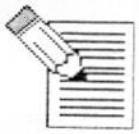
Resource ReSerVation Protocol

Resource ReSerVation Protocol (RSVP) is a type of network resource reservation. RSVP reserves bandwidth and other resources on routers located throughout a network for a transmission path. All routers in the network path must be RSVP-compliant for this priority. RSVP is allocated on a first-come, first-served basis and ties up the amount of bandwidth needed for processing an application. RSVP depends on a router's Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) decision-making for transmission.

Figure 9: Resource ReSerVation Protocol



Notes

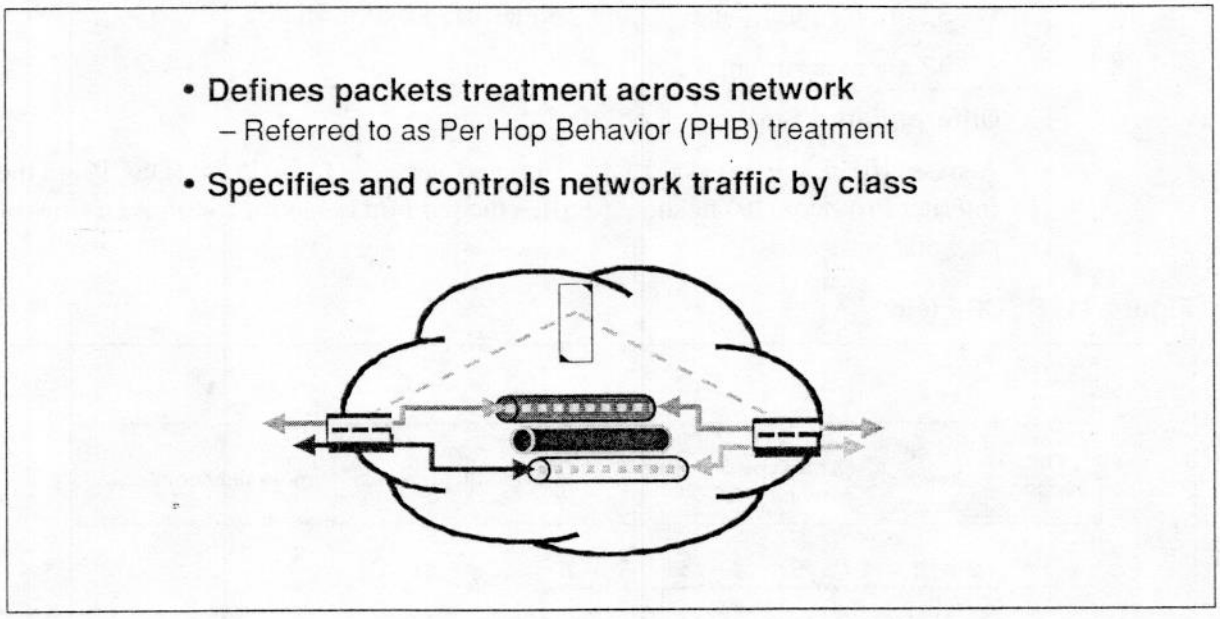


Differentiated Services

Differentiated Services (DiffServ) is a type of packet prioritization.

DiffServ enables you to specify and control network traffic by class so that certain types of traffic get precedence; for example, voice traffic, which requires a relatively uninterrupted flow of data, can get precedence over other kinds of traffic. It is also an effective method to maintain QoS when a company has a combination of Layer 2 and Layer 3 switches.

Figure 10: Differentiated Services



Notes

Class of Service

DiffServ is the most advanced method for managing traffic in terms of what is called Class of Service (CoS). Unlike the earlier mechanisms of 802.1p tagging and Type of Service (ToS), DiffServ avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet.

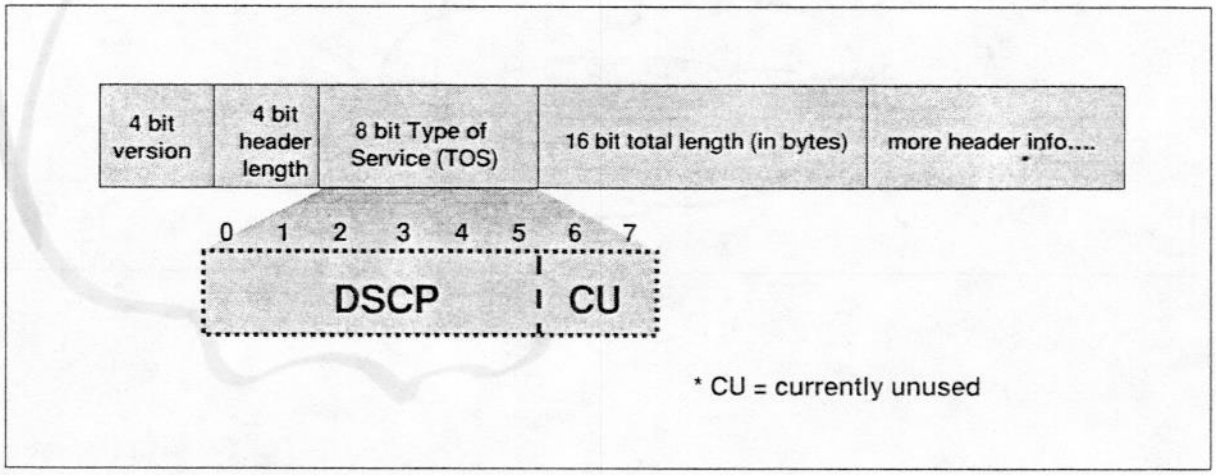
For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors. Of these fields:

- 32 are for public use (21 are standardized by the IETF)
- 32 are experimental

Differentiated Services Code Point Field

A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (IP) header specifies the per hop behavior for a given flow of packets.

Figure 11: DSCP Field



Notes

Class Selector (CS)

The Class Selector (CS) of DiffServ behavior is represented by eight priority classes and uses the same bit positions as the IP Precedence field in ToS. The classes are numbered from CS0 to CS7. CS7 has the highest priority. CS0 is equivalent to best-effort service.

Expedited Forwarding and Assured Forwarding

Expedited Forwarding (EF) and Assured Forwarding (AF) allow you to prioritize VoIP traffic and signaling.

EF provides a low-latency, high-priority service that is suited for VoIP.

AF consists of four different service classes, each with three different discard-priority levels. Class 4 has priority over Class 3, and so on.

Notes

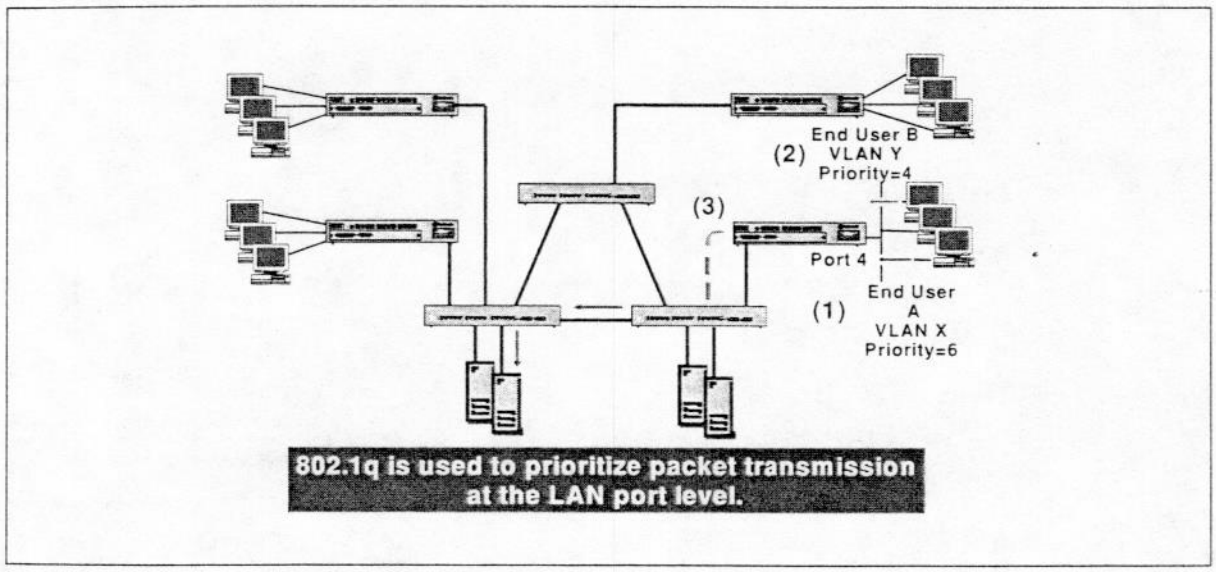
Ethernet 802 Standards

Congestion management defines how different queuing categories, such as Ethernet 802 standards 802.1p and 802.1Q, prioritize packet transmission. 802.1p and 802.1Q define prioritization of traffic within a LAN. In defining these standards, 802-type priority traffic is processed and placed in front of less critical business traffic. 802.1p is the level assigned at the user level, while 802.1Q is assigned at the LAN port level.

Ethernet 802.1Q

Ethernet 802.1Q is an Institute of Electrical and Electronics Engineers (IEEE) Ethernet standard that adds four additional bytes to the standard 802.3 Ethernet frame for Ethernet QoS and Virtual LAN (VLAN) support. Most Ethernet switches support the 802.1Q standard, with the exception of perhaps the least expensive ones.

Figure 12: Ethernet 802.1Q



Notes

Ethernet 802.1Q prioritizes packet transmission at the LAN port level:

- Untagged frames from End User A and End User B arrive simultaneously at port 4 of a switch.
- Port 4 has a priority value of 6 for VLAN X (End User A) and a priority value of 4 for VLAN Y (End User B). If End User A frames exit the switch on an 802.1Q tagged port, exiting End User A frames would also be 802.1Q tagged, including the 802.1p user priority of 6.
- End User A frames are sent before End User B frames.

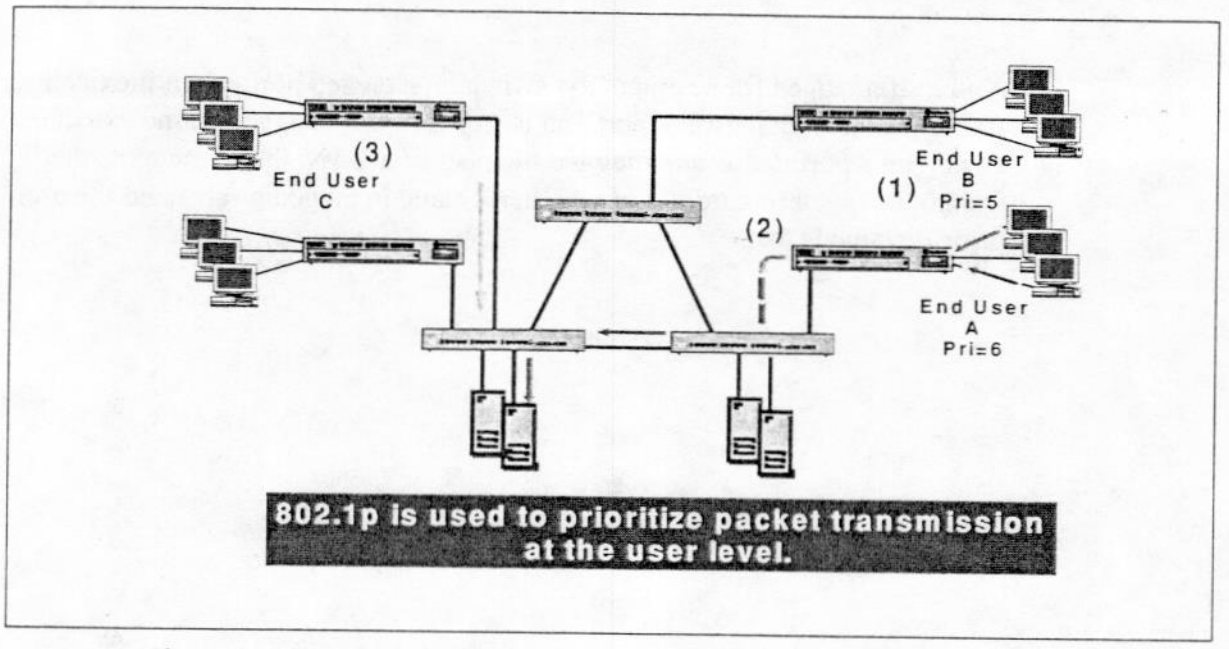
Note: If a tagged frame enters the switch on a tagged port, when it exits the frame retains both tags, the port and user priority. If a tagged frame exits the switch on a port that is an untagged member of a LAN, the frame exits the switch untagged (regardless of whether it came in tagged or not) and the user priority value is lost.

Notes

Ethernet 802.1p

Ethernet 802.1p (802.1p) is an effective method to maintain QoS when a company has a combination of Layer 2 and Layer 3 switches. The Ethernet QoS is accomplished through the three 802.1p user priority bits. The 802.1p user priority bits allow you to create eight classes of service for packets that cross Ethernet networks. Based upon the 802.1p value, each packet is placed in the correct queue.

Figure 13: Ethernet 802.1p



Notes

Ethernet 802.1p prioritizes packet transmission at the user level:

- Frames for End User A and End User B arrive simultaneously at the switch for transmission. End User A frames have a priority of 6, while End User B frames have a priority of 5.
- Based on priority levels, End User A frames are processed first, while End User B frames are queued and transmitted when End User A transmission is complete.
- Frames for End User C are not assigned a priority. The frames are transmitted after the prioritized frames.

Note: If this network policy is assigned in the entire network, this will be true on all switches.

Notes

Port-based Prioritization

Port-based Prioritization is an effective method to achieve optimal voice quality. With Port-based Prioritization, you can prioritize all traffic coming from the specific port of an Ethernet Layer 2 switch. In this case, 802.1p is not required, because you are prioritizing all traffic coming in on this port.

If the device attached to the Layer 2 switch port is an IP phone, then port prioritization is not recommended since IP terminals can be unplugged and moved. If a PC is connected to a port configured to use port prioritization, then all of the PC's traffic is given high priority treatment.

Protocols

Products can use UDP port ranges to provide high priority to VoIP packets as a form of QoS in existing legacy IP networks. The same port ranges must be reserved and set to high priority on all routers where an administrator expects to have QoS support. DiffServ networks do not require a reservation of port ranges. You can designate any port range that is not used by well-known protocols and applications. Each H.323 or VoIP RTP flow uses two ports for each direction. The total number of UDP port numbers to be reserved depends on how many concurrent RTP flows are expected to cross a router interface.

Guidelines

Remember the following guidelines:

- Backbone routers reserve more ports than edge routers
- Port ranges on edge routers are a subset of backbone router port ranges
- Two ports must be reserved for each call expected to be carried over WAN link

Note: H.323 is a packet-based signaling standard that provides a foundation for audio, video, and data communications across IP-based networks. See the "VoIP Standardization and Signaling Protocols" lesson, later in this course.

Notes

Traffic Separation

Traffic Separation is an optional technique.

If all Ethernet switches support the Ethernet 802.1Q standard for VLANs, then Traffic Separation with VLANs enables you to place all voice traffic onto one VLAN and all other data traffic on another VLAN.

Benefits of Traffic Separation are:

- Enables you to ensure voice QoS by allowing voice VLAN traffic to have a higher priority over the data VLAN traffic
- Provides an easy way to connect a VoIP gateway from an IP-enabled switch to the company's existing Ethernet Layer 2 switch using only Layer 2 technology

Caution: *Not all vendors recommend the use of VLAN. Use of VLAN depends upon the customer requirements.*

Internet Protocol Address Prioritization

VoIP traffic can also be prioritized by its IP address. This approach is ideal for devices with static IP addresses that rarely, if ever, change. IP Private Branch Exchanges (PBXs), VoIP gateways, and call servers are VoIP devices that can have static IP address assignments. A network administrator can configure the routers to filter (classify) and prioritize all packets originating from these IP addresses and know they are from VoIP devices.

Notes

Packet Fragmentation

In mixed voice and data IP networks, packets must be fragmented prior to traversing bandwidth-limited (less than 1 Mbps) connections to minimize voice delay and jitter. There are several different protocols that can be used to fragment packets.

Tip: *There are two types of fragmentation that are more universal and not limited to a specific link layer technology such as ATM or Frame Relay FR.12. These methods are via the PPP protocol and via IP fragmentation.*

Frame Relay FRF.12

For Frame Relay connections, you can use the FRF.12 standard for fragmenting packets.

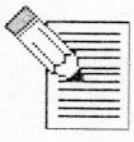
Point to Point Protocol Fragmentation and Interleaving

Many routers support PPP Fragmentation. PPP Fragmentation splits large packets into multiple smaller packets and encapsulates them into PPP frames before queuing and transmission. PPP Fragmentation allows higher-priority VoIP packets to interrupt and transmit ahead of the larger, lower priority packets that have already been queued. The packets can be interleaved, so the maximum delay a voice packet experiences is one packet time.

Asynchronous Transfer Mode

ATM natively provides fragmentation. ATM packets are fragmented into 53-byte cells.

Notes



IP Fragmentation (Maximum Transmission Unit)

Most routers use a default maximum packet size of 1500 bytes, which can take a considerable amount of time to transmit over a low bandwidth connection.

Consider a 1,500-byte data packet being transmitted over a 64 Kbps connection. It takes 188 ms to transmit this data packet out of the router onto the 64 Kbps connection. This same queuing delay is added again as the packet is queued in at the far end router on the other side of the connection.

Data packets use up almost all of the delay budget for the voice traffic before the first voice packet is ever transmitted. Reducing the MTU can put more data on the WAN sooner and is not necessarily as efficient. There is a trade-off between better network performance and voice quality. See the section titled "Maximum Transmission Unit" for additional information.

Notes

Challenges of Low Speed Wide Area Network Connections

There are a number of items to consider when using routers with low bandwidth WAN and access network connections.

Serialization Delay

Serialization delay can occur when a small packet has to wait for a large packet to be sent over the link. This can result in end-to-end delay (latency) and variable delay (jitter). For example, when transporting smaller packets over a network infrastructure that typically has larger packets of up to 1,500 bytes, the larger packets can introduce variable delay (jitter) in the network and impact the voice quality.

In a WAN environment where link speeds are low compared to the LAN, link speeds less than 1 Mbps are subject to serialization delay. See the figure below for details.

Figure 14: Serialization Transmission Delay for Different Link Speeds

Serialization transmission delay in msec. for different link speeds										
Link Speed in Kbps	Packet Size									
	40 bytes	80 bytes	88 bytes	136 bytes	184 bytes	232 bytes	280 bytes	520 bytes	1K bytes	1.48K bytes
56	5.714	11.429	12.571	19.429	26.286	33.143	40.000	74.286	146,286	211.429
64	5.000	10.000	11.000	17.000	23.000	29.000	35.000	65.000	128.000	185.000
128	2.500	5.000	5.500	8.500	11.500	14.500	17.500	32.500	64.000	92.500
256	1.250	2.500	2.750	4.250	5.750	7.250	8.750	16.250	32.000	46.250
384	0.833	1.667	1.833	2.833	3.833	4.833	5.833	10.833	21.333	30.833
1000	0.320	0.640	0.704	1.088	1.472	1.856	2.240	4.160	8.192	11.840
1540	0.208	0.416	0.457	0.706	0.956	1.205	1.455	2.701	5.319	7.688
2048	0.156	0.313	0.344	0.531	0.719	0.906	1.094	2.031	4.000	5.781
10000	0.032	0.064	0.070	0.109	0.147	0.186	0.224	0.416	0.819	1.184
100000	0.003	0.006	0.007	0.011	0.015	0.019	0.022	0.042	0.082	0.118
150000	0.002	0.004	0.005	0.007	0.010	0.012	0.015	0.028	0.055	0.079

Notes

Link Speed / 8 (or ÷ by 8)

70 ← 56K

MTU = S/D (Link Speed)

Link Speed = 8 / MTU x 8 / S/D

S/D Serialization Delay = MTU x 8 / Link Speed

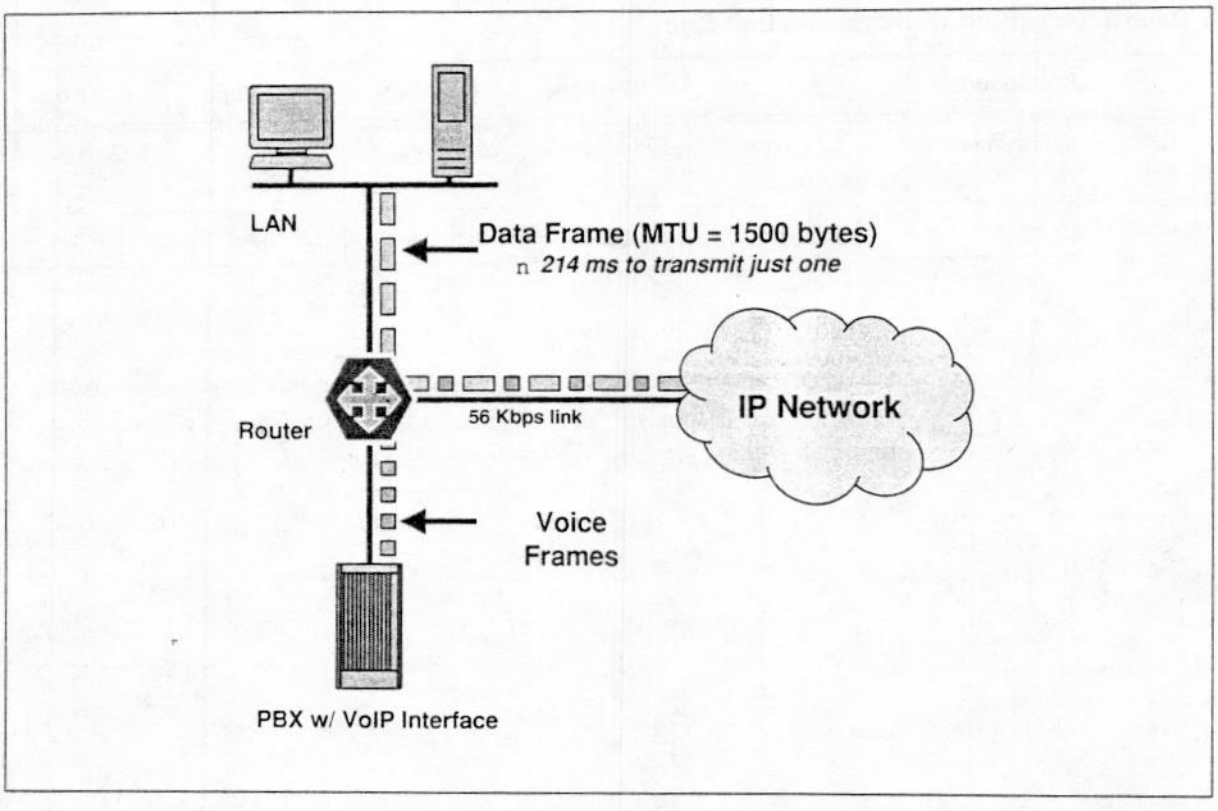
(136 bytes) x 8 / 56 K bps = 19.429 ms

Serialization Delay = MTU x 8 / Link Speed.

Maximum Transmission Unit

The Maximum Transmission Unit (MTU) is the maximum amount of bytes carried by any packet. When the access line is running at a low speed, smaller packets must wait behind the larger packets.

Figure 15: Maximum Transmission Unit



Notes

Maximum Transmission Unit Sizes

A possible solution is to begin with an MTU size of 256 bytes for connections less than 1 Mbps and adjust upward, as needed. The table below shows the recommended maximum MTU sizes for different connection speeds.

Table 2: Maximum Transmission Unit Sizes

Link Speed	56 Kbps	64 Kbps	128 Kbps	256 Kbps	512 Kbps
Recommended Maximum MTU	128 bytes	128 bytes	256 bytes	512 bytes	1024 bytes
Ideal MTU	70 bytes	80 bytes	160 bytes	320 bytes	640 bytes

Caution: *Remember, reducing the MTU can put more data on the WAN sooner and is not necessarily as efficient. There is a trade-off between improved network performance and voice quality.*

Notes

Key Infrastructure Requirements

Local Area Network Environment

Half-Duplex Versus Full-Duplex Ethernet Connections

Half-duplex is the term used to describe alternating transmissions over a communications link. Each station can either transmit or receive, but cannot do both simultaneously. Full-duplex data transmission is defined as the ability for communications to flow both ways simultaneously over a communications link. In Ethernet or Fast Ethernet networks, the collision detection and avoidance protocol is turned off and frame transmission occurs in both directions at the same time, doubling the available bandwidth on a link.

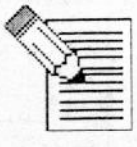
Autonegotiation

Autonegotiation is standard for Fast Ethernet. This standards enables two devices that share a common link to advertise their speed and duplex mode capabilities, acknowledge receipt and understanding of shared modes of operation, and reject modes of operation that are not shared. This allows the devices to leverage the maximum resources of each node.

There are some things to watch for with autonegotiation. For autonegotiation to work, both sides must support autonegotiation. Occasionally customers will run into devices with outdated network interface card drivers that either do not support autonegotiate or incorrectly implement autonegotiate. After several attempts to make a connection, the link may stop trying to connect so that no communication occurs. Or perhaps the link is incorrectly established, such as 10 Mbps on one end and 100 Mbps on the other end, or full-duplex on one end and half-duplex on the other end.

To correct this type of mode mismatch problem, it may be necessary to disable autonegotiation and set a fixed speed and duplex mode for the local port (10 Mbps or 100 Mbps, half- or full-duplex) so that the modes coincide with the operating capabilities of the remote link.

Notes



Layer 3 Switches

Layer 3 switches, also known as routing switches, combine the speed of a switch with the IP routing capability of a router. Traditional routers store their routing instructions in software. Layer 3 switches store their routing instruction in hardware. This allows Layer 3 switches to reduce latency by routing millions of packets per second.

Tip: *If a customer has a combination of Layer 2 and Layer 3 switches, 802.1p and DiffServ are effective methods to maintain toll quality QoS.*

Power Management

Building power management into the IP network is important for increasing reliability of the VoIP network. Some ideas for implementing power management in your network:

- Power over LAN (sometimes called inline power) for IP terminals
- Redundant power supplies for the network equipment
- Uninterruptible Power Supply (UPS)
- Sufficient cooling in wiring closets

Note: If you have redundant power supplies, plug each power supply into a separate UPS. If possible, have each UPS on its own circuit. If one circuit fails, the other circuit still has power.

Notes

Common Data Protocols and Applications

Common data protocols and applications include:

- **File Transfer Protocol (FTP):** Used to exchange files between computers. FTP can be used to transfer very large files and can be very bandwidth intensive.
- **Telnet:** Used to access other computers over TCP/IP. It is not very bandwidth intensive.
- **Simple Mail Transfer Protocol (SMTP):** Used to queue messages on a mail server. SMTP can be very bandwidth intensive.
- **Hypertext Transfer Protocol (HTTP):** Used by computers accessing web pages. This can be bandwidth intensive depending on what the user is accessing.
- **Structured Query Language (SQL):** Used to query information from a relational database, such as Oracle or Sybase. SQL is a very talkative protocol that should preferably be kept to one VLAN.
- **Domain Name Server (DNS):** Used by computers to discover the IP address associated with a computer's host name, or a name to go with an IP address.
- **Dynamic Host Configuration Protocol (DHCP):** Used by computers to gather their initial network configuration information, such as host name, gateway, and subnet mask. It is not that talkative.

Lack of Quality of Service in 802.11 Wireless Environment

Wireless networks typically have longer delay then traditional media. The industry is still looking for ways to provide QoS on wireless networks.

Notes

Wide Area Network Environment

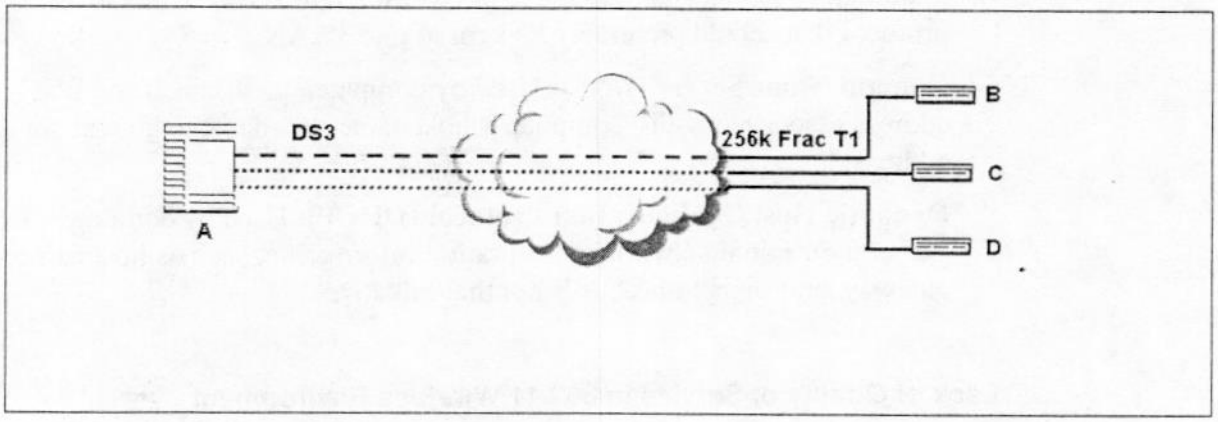
Importance of Quality of Service

The same traffic queue management issues relevant on the LAN apply to the WAN, though with far greater complexity. The issue over WAN links, unless they are privately managed, is how much control your organization maintains once traffic leaves your private network for public connections.

The WAN presents a challenge to guarantee consistent application performance because it has so many scenarios.

For example, in a Frame Relay environment, a typical design can have many low-speed links that terminate at branch locations with high-speed links. The low-speed links can be overrun by traffic from the central site with a larger bandwidth connection.

Figure 16: High-Speed Link Terminating in Low-Speed Links



Notes

Evaluating Customer Routers

There are three factors that influence router performance:

- Baseline speed of a router:
  - Performance of router, given the most favorable conditions
- Characteristics of the routed traffic:
  - Packets that arrive in bursts are delayed more than evenly-spaced packets.
- External events (besides routed traffic):
  - Interaction with other network devices
  - Routing table maintenance
  - Address resolution

Need for Call Admission Control

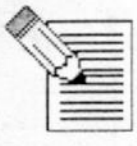
In networks with a high proportion of voice traffic, Call Admission Control (CAC) can prevent congestion by limiting the number of calls that can be active through various nodes in the network. With no CAC, when the number of calls increases above the recommended utilization, the voice quality in the network declines.

For example, if the WAN access link between the two Private Branch Exchange (PBX) systems has the bandwidth to support only two VoIP calls, admitting the third call impairs the voice quality of all three calls. CAC allows a gateway to reject traffic once a defined threshold is reached on the gateway. After the call is rejected, the originating gateway must find another means of handling the call. There are several possibilities, most of which are dependent on the configuration of the gateway.

Lack of Quality of Service in Frame Relay Environment

Frame Relay networks provide no form of QoS other than the ability to mark traffic as Discard Eligible (DE). All traffic not marked DE receives the same treatment within a customer's Committed Information Rate (CIR).

Notes



Security Issues

Firewalls are designed to protect the internal network from the outside network. The design of a firewall can go from relatively simple firewalls that come preconfigured, to complex designs that incorporate multiple firewalls and proxy servers. For a firewall to work with VoIP, certain "holes" punched in the firewall for the VoIP ports or the firewall must understand the protocols going across the firewall, such as RTP, H.323, SIP, etc. Even if the firewall understands the VoIP protocols that a customer is using, it does not ensure that the customers will be able to call customers outside the firewall.

Network Address Translations (NATs)

Network Address Translations (NAT) permits a few IP addresses to be shared by many users. It also permits the connection of an intranet-based address (for example, 10.0.0.1) from accessing the internet. If either party of a call uses NAT there can be a problem creating a call because the IP information is not only written in the IP header that gets exchanged by the NAT server, but also deeper in some packets, for example SIP packets. Some newer NAT servers and firewalls are being developed that understand RTP, H.323, and SIP, but older ones may not.

Encryption

One solution that allows voice traffic to cross a firewall and also avoid the issues raised by NAT is to create a VPN where both machines are on the same VPN network. Therefore, traffic is tunneled through firewalls. This may cause added delay, however, making VoIP unusable.

Notes

Common Ethernet Network Issues for LAN Environment

Bandwidth

VoIP requires bandwidth of 10/100 Ethernet switching.

Tip: *For low-bandwidth (less than 1 Mbps) connections, it is recommended to use no more than 50 percent of the available bandwidth for voice traffic. For connections greater than 1 Mbps, you can use up to 85 percent of the available bandwidth for voice traffic.*

Compression

There are several possible choices for voice compression. The ITU G.729 CODEC generally provides the lowest bandwidth with the highest voice quality. G.729 compresses the voice call from approximately 64 Kbps to 8 Kbps. This 8 Kbps is the raw-voice bandwidth and needs to be encapsulated into other protocols before it becomes VoIP and can be transported over an IP network. The link layer protocol to transport the IP packet could be PPP, Frame Relay, or ATM. The additional overhead added by these protocols increases bandwidth required for VoIP packets to approximately 20 to 28 Kbps.

Remember, bandwidth requirements are estimates, and vary per product or packetization parameter settings.

Tip: *Voice compression is not required over high bandwidth, Ethernet connections.*

Notes

Delay

The overall delay budget for a voice call, from the time you speak until the time the receiver hears your voice, must typically be no longer than 150 ms for good quality voice over landline connections.

Congestion

Ethernet networks require less sophisticated QoS mechanisms than low-bandwidth WAN connections because the bandwidth is much higher resulting in significantly lower queuing and network delay. However, network congestion, even for short periods of time, and bursty, TCP-based Internet traffic can cause significant voice quality problems if QoS is not applied.

Note: Only use switched-media Ethernet networks with VoIP. Never use shared-media Ethernet hubs. QoS mechanisms, such as 802.1p, VLANs, and port prioritization, can be used for VoIP traffic over Ethernet networks. If the Ethernet switches support Layer 3 capabilities, then QoS mechanisms, such as DiffServ and IP address prioritization, can also be used.

Notes

Collision

In an Ethernet environment, collisions occur more frequently as utilization levels increase. This can cause unpredictable delays between packets due to the access protocols associated with Ethernet LANs, where a random exponential back-off algorithm is used after a collision is detected.

If utilization level exceeds 50 percent, voice-encoded packets generally will flow to the router for transmission on the Intranet, with unpredictable delays between packets.

At a minimum, Layer 2 switching is required to avoid network collision.

Packet Reordering

In some cases there can be multiple paths for a VoIP packet to take when traveling from its source to its destination. If all VoIP packets do not take the same path, then packets can arrive out of order. This can cause voice quality issues; however, packet reordering often has little or no adverse impact to data traffic quality.

Notes

Practice

Answer the following questions.

1. What is a benefit of Traffic Separation using VLANs?

   - Enable you to ensure via QoS by allowing voice VLAN traffic to have a high priority over the data VLAN traffic
   - Provides an easy way to connect a VoIP gateway from an IP enabled switch to the company's existing Ethernet layer 2 switch using only layer technology

2. How does Port-Based Prioritization achieve optimal voice quality?

   Prioritize an entire section port of traffic

3. Ethernet 802.1p is required for Port-Based Prioritization.

   give CoS

   a. True
   b. False

4. Frame Relay FRF.12 natively provides fragmentation since all packets are fragmented into 53-byte frames.

   a. True
   b. False

Notes

5. What is the difference between Expedited Forwarding and Assured Forwarding DiffServ classes?

EF high-Priority service

AF priority for classes (4 classes) levels

6. What is the recommended Maximum MTU for VoIP at 256 Kbps?

512 bytes

7. List three ideas for implementing power management in your network.

- Redundant Power [illegible] for the network equipment
- UPS
- Sufficient outlets in wiring closets

Notes

Answers to Practice

If you successfully completed the Practice and are confident of your understanding of the material, you have satisfied the lesson requirements

Notes

Summary

In this lesson, you learned the distinction between the various methods available for implementing QoS prioritization of VoIP traffic in order to achieve the best voice quality. You have an understanding of the challenges of running VoIP over low speed WAN connections. You learned about the infrastructure needed to support VoIP traffic in the LAN and WAN environment and the common Ethernet problems associated with this traffic.

Notes

Notes

VoIP Standardization and Signaling Protocols

Introduction

The Internet is a popular and widely used communications network. It uses Internet Protocol (IP), the most scalable, flexible network technology capable of working across any network infrastructure. IP is a universal communications language that provides the foundation to allow dissimilar physical networks and equipment from a variety of vendors to interconnect. IP allows computers to share resources across networks and application protocols that support communication services, such as the World Wide Web (WWW). Computers understand IP without a translator, which can allow them to function as a coordinated unit with an IP network.

A relatively new technology that utilizes the IP network is Voice over IP (VoIP). VoIP provides real-time communication and requires a greater QoS and more bandwidth than most applications. VoIP uses packet-switched connections to transmit real-time two-way voice traffic, faxes, and other information. These transmissions have traditionally been processed through the dedicated circuit-switched connections of the Public Switched Telephony Network (PSTN).

For communications to be successfully transported over the IP network, standards exist that utilize signaling protocols to accomplish this task. These standards have been determined and introduced by organizations specifically designated to define communications standards for transmission of voice, video, and data. In this lesson, we will review the VoIP standards and networking protocols that support the transport of communications across IP-based networks.

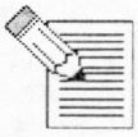
Notes

Objectives

Given this module and the instructor's presentation, you will be able to complete these tasks:

- List organizations instrumental in defining and developing Voice over Internet Protocol (VoIP) standards
- Identify the role H.323 plays within a VoIP network
- Apply H.323 standards to a VoIP environment during call setup implementation
- Identify the role of Session Initiation Protocol (SIP) in IP Telephony
- Recognize the role of SIP in supporting multimedia sessions with IP Telephony
- Differentiate the benefits and functionality of SIP versus H.323 within a VoIP network
- Identify other standards that support communications transmission within a VoIP network

Notes



Standards and Organizations

Standards are extremely important when transmitting communications throughout an IP network. The basis of a network is allowing equipment and applications to transport, recognize, process, and respond to user requests for information. Some advantages of standards are:

- **Interoperability:** Equipment can interconnect and operate properly
- **Competition:** Manufacturers can focus on their respective product, equipment, or application strengths
- **Ready Market:** Development of equipment that can function in an open network
- **Obsolete Technology:** Users are protected from the introduction of technology that can become obsolete in a short period of time

Notes

Standards Organizations

Within the communications industry, several organizations exist that help determine and define standards. Some key players are:

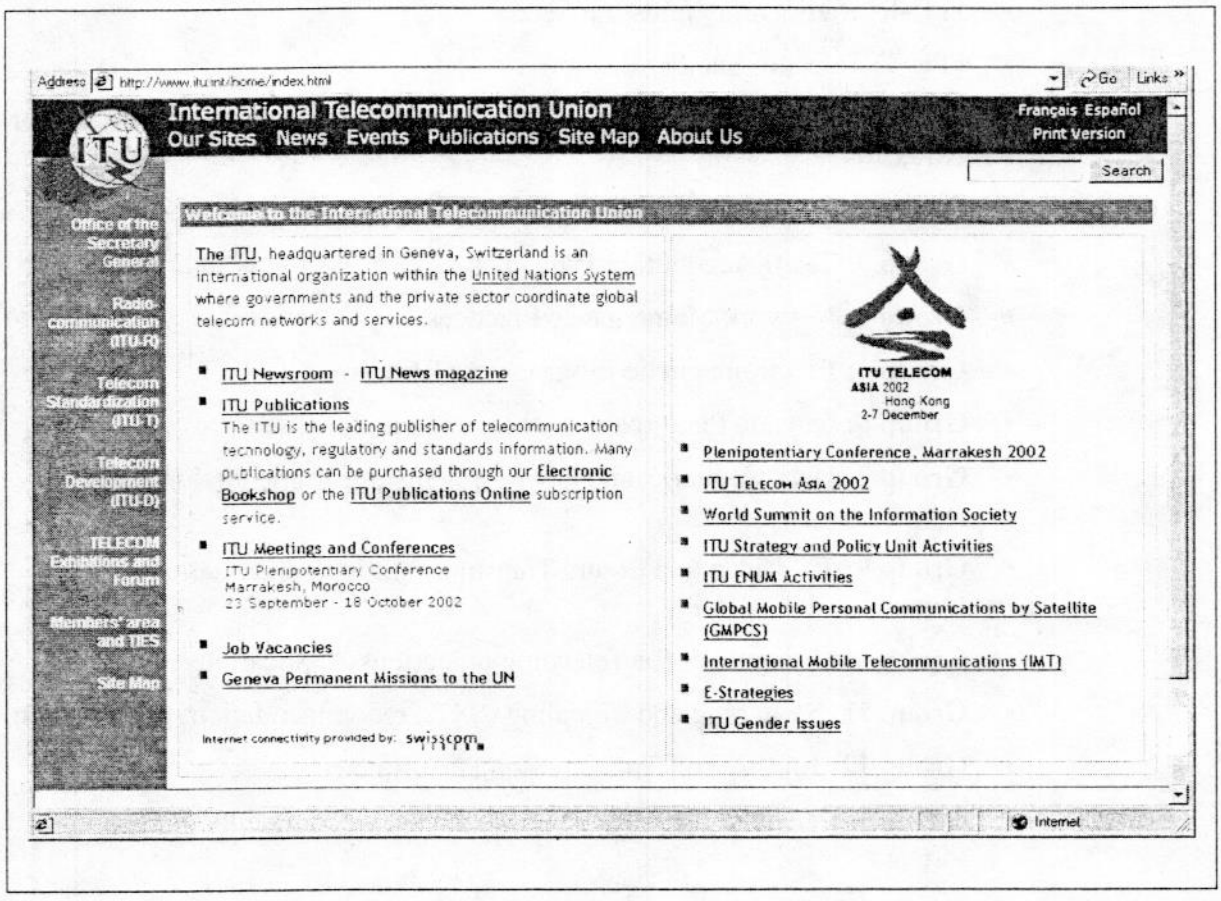
- **American National Standards Institute (ANSI):** Authorizes industry organizations to develop actual technical standards; T-1 committee develops all network provider standards (www.ansi.org)
- **International Standards Organization (ISO):** Developed the ISO model, JPEG, MPEG, and many international quality standards (www.iso.ch)
- **International Telecommunications Union (ITU):** Develops standards that allow international network providers to interconnect (www.itu.int)
- **European Telecommunications Standards Institute (ETSI):** Responds to member needs for standardization (www.etsi.org)
- **Institute of Electrical and Electronic Engineers (IEEE):** Develops standards for the electrical industry; developed 802.X LAN/MAN standards (www.ieee.org)
- **Electronic Industries Alliance (EIA):** Dedicated to consumer electronic standards; sanctioned by ANSI; a key player in HDTV and multimedia standards (www.eia.org)
- **Information Infrastructure Standards Panel (IISP):** Promotes, accelerates, and coordinates standards for a National Information Infrastructure, the "Information Superhighway"; sponsored by ANSI
- **Telecommunications Industry Association (TIA):** The official standards body for cellular/PCS; heavily involved with defining VoIP standards (www.tiaonline.org)
- **Internet Engineering Task Force (IETF):** Provides Internet standards (www.ietf.org)

Two key players in the IP network world are the ITU and the IETF. The organization and recommendations they provide affect transport of information.

International Telecommunications Union

The ITU is an international organization that supports the determination of standards used in a voice, video, and data network. However, many standards are designed and recommended by an organization outside of ITU, such as ANSI, and later incorporated into ITU-T recommendations, such as V.28.

Figure 1: International Telecommunications Union Home Page



Notes

The ITU actually consists of several committees dedicated to a specific aspect of the industry. Within each committee, a study group is formed, which then releases recommendations for standards. The standards are issued by a letter (V, X, G, and so forth) representing the study group assigned to a specific activity followed by a sequence number. The specific ITU committees are:

- **ITU-D:** Telecom Development
- **ITU-R:** Radiocommunication Sector
- **ITU-T:** Telecom Standardization

Within the ITU-T, there are 15 study groups that prepare recommendations for standards:

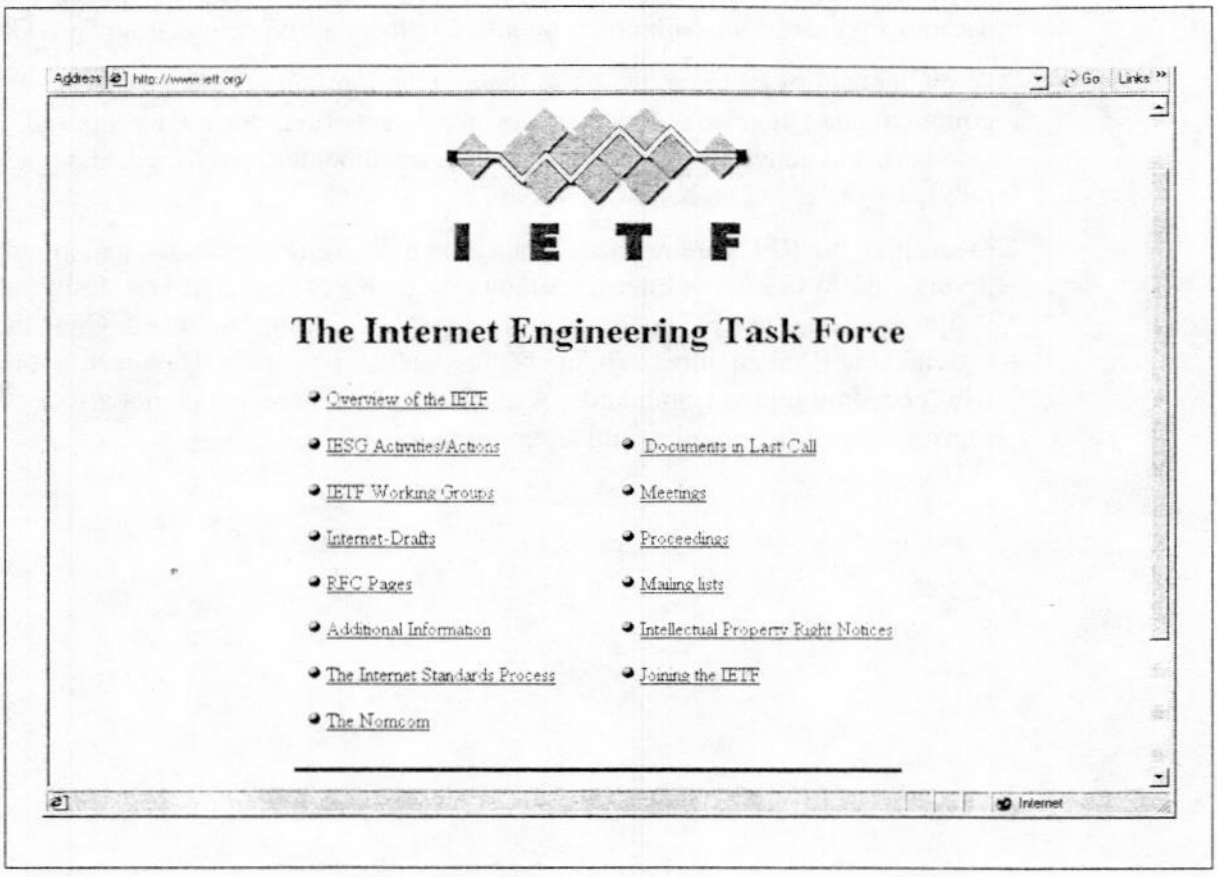
- **Group 2:** Network Operation and Study Group QoS
- **Group 3:** Tariff Accounting Principles
- **Group 4:** Network Maintenance Practices
- **Group 5:** Electromagnetic Environment Effects
- **Group 6:** Outside Plant (cables, poles and vaults)
- **Group 7:** Data Networks and Open Systems; recommendations in X. format
- **Group 9:** TV Video and Sound Transmission; recommendations in H. format
- **Group 10:** Languages for Telecommunications Applications
- **Group 11:** Switching and Signaling (SS7); recommendations in Q. format
- **Group 12:** End-to-End Transmission Performance
- **Group 13:** General Network Aspects (ISDN); recommendations in I. format
- **Group 15:** Transmission Systems (DS-1; SONET); recommendations in G. format
- **Group 16:** Modem, Data, Telegraph; recommendations in V. format
- **Special Study Group:** International Mobile Telecommunications (IMT) 2000 and beyond

The ITU releases Recommendations that generally become network standards as the recommendations are accepted and implemented by manufacturers, providers, and suppliers.

Internet Engineering Task Force

The function of the IETF is to develop and review specifications intended as Internet Standards. Its tasks are accomplished through the use of more than 100 working groups, organized by topic into several areas, such as routing, transport, and security. IETF membership is comprised of network designers, operators, vendors, and researchers.

Figure 2: Internet Engineering Task Force Home Page



Notes

The IETF is comprised of:

- **Internet Engineering Steering Group (IESG):** Comprised of Area Directors that manage IETF working groups
- **Internet Architecture Board (IAB):** Provides architectural oversight and arbitrates appeals

The IETF releases Request for Comment (RFC) documents that can range from an official Internet standardized protocol specification to research results. Various organizations with common interests form a "Working Group" (WG).

A WG generates RFCs and submits them to the Internet community for comment and suggestion. Once an RFC reaches its final draft, the proposed standard, and generally agreed-upon idea, is documented, published, and made public by the IESG on behalf of the IETF.

Over time, the RFCs are refined. When a final document is created and agreed upon by the WG and the Internet community, a vote is taken. After a six-month waiting period, the RFC becomes ratified and becomes the standard. Once the official vote is taken, most vendors begin to develop product. However, not all RFCs become Internet Standards. A number of RFCs created do not affect transporting of information and are informational RFCs.

Notes

Signaling Protocols

Signaling protocols initiate and control communications. The type of protocol and the technology involved to support it is dependent on the type of communications and applications involved, such as voice, video, or data. The signaling protocols that will be addressed are:

- H.323
- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- MEGACO/H.248 —> IEEE/ITU

Notes

H.323

H.323 is a suite of protocols that initially supported only videoconferencing systems over LAN/WAN topologies and protocols. However, H.323 V2 has evolved into a packet-based signaling standard that provides a foundation for audio, video, and data communications across IP-based networks, including the Internet. H.323 is network, platform, and application independent, allowing any H.323 compliant device to interoperate with any other. Though H.323 does not provide a guaranteed QoS, users can communicate without concern for compatibility. H.323 supports both stand-alone devices and embedded personal computer technology, in addition to point-to-point and multipoint conferencing. H.323 also addresses:

- Call control
- Multimedia management
- Bandwidth management
- Interfaces between LANs and other H.323 non-compliant endpoints

Table 1: H.323 V2

Component	Description
Network	Non-guaranteed bandwidth packet switched networks, (Ethernet)
Video	H.261 H.263
Audio	G.711 G.722 G.728 G.723 G.729
Multiplexing	H.225
Control	H.245
Multipoint	H.323
Security	H.235
Data	T.120
Comm. Interface	TCP/IP

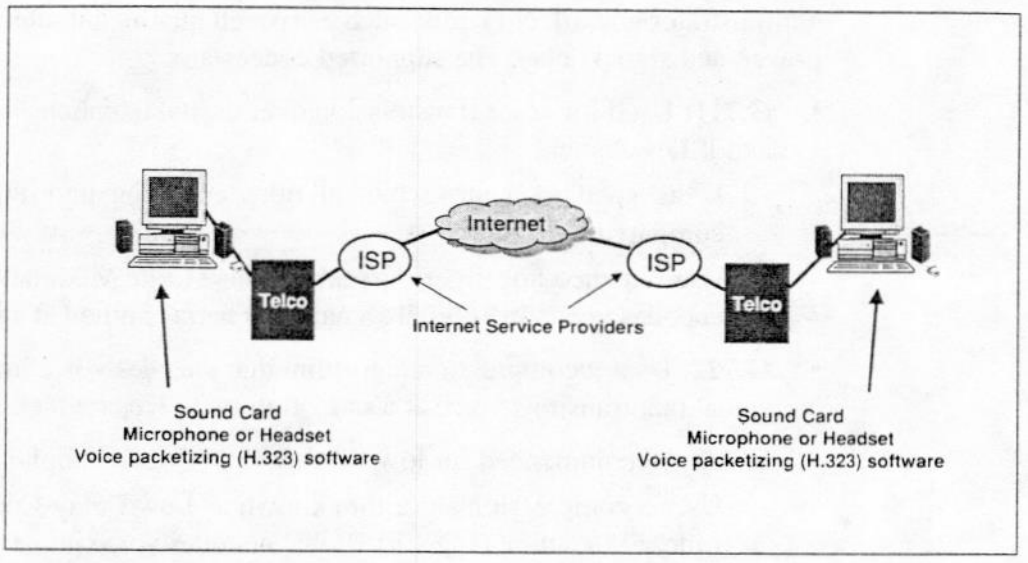
Note: G.XXX compression algorithms are existing ITU standards incorporated into the H.323 protocol suite.

H.323 incorporates support for various CODECs or speech compression techniques for digitizing and compressing speech signals derived from the existing ITU standards. These CODECs are chosen by the network administrator and affect factors, such as speech quality, bit rate, computer power, and signal delay. The supported codecs are:

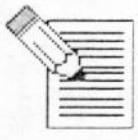
- **G.711:** Used for voice transmission over digital telephone sets on a PBX and ISDN channel
  - Is the standard against which all other encoding algorithms are compared
  - Uses an encoding algorithm called Pulse Code Modulation (PCM) that encodes voice into digital signals that is transmitted at a rate of 64 Kbps
- **G.722:** Uses a compression algorithm that encodes voice into a digital signal that transmits voice at a rate of up to 32 Kbps
- **G.728:** Recommended for low-bit-rate ISDN video telephony
  - Uses a compression algorithm known as Low Delay-Code Excited Linear Prediction (LD-CELP) that encodes voice into a digital signal that transmits voice at a rate of 16 Kbps
- **G.723.1:** Uses a compression algorithm that encodes voice into a digital signal that transmits at a low rate of 5.3 or 6.3 Kbps
- **G.729:** Default specification for Internet Telephony
  - Uses a compression algorithm known as Conjugate Structure-Algebraic Code Excited Linear Prediction (CS-ACELP) that encodes voice into a digital signal that transmits at a rate of 8 Kbps
  - Utilizes silence suppression or Voice Activity Detection (VAD) in the transmission of voice communications which can further reduce bandwidth requirements to as low as 4 Kbps

Notes

Figure 3: H.323-based Software Supports VoIP PC Calls



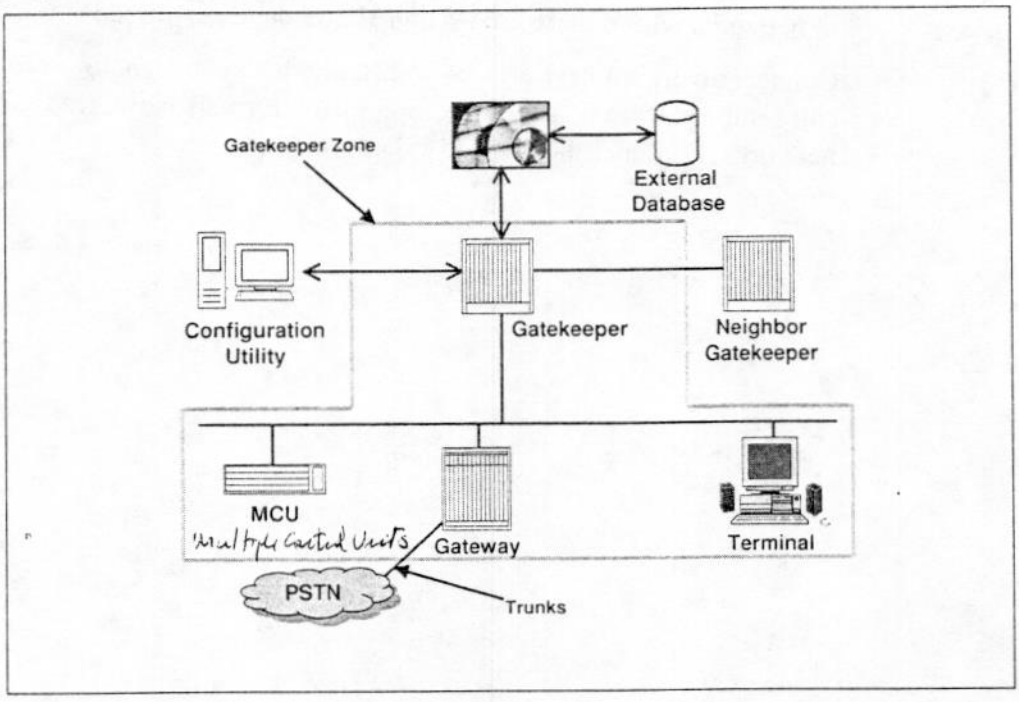
Notes



Components of H.323

H.323 is a flexible standard that can be applied to voice-only handsets and full multimedia video-conferencing stations. H.323 has broad industry support, which has established H.323 as the standard for transporting audio and video communications in an IP packet-based network. H.323 consists of four key components for an H.323-based communications system: Gateway, Gatekeeper, Multipoint Control Unit (MCU), and Terminals.

Figure 4: H.323 Architecture Overview



Note: A gatekeeper zone is comprised of terminals, gateways, and MCUs managed by a single gatekeeper.

Notes

Gateways

Some characteristics of gateways are:

- Optional in an H.323 conference
- Bridge H.323 conferences to other networks, communications protocols, and multimedia formats
- Not required if connection between two H.323 devices on the same LAN or in networks where there are no non-H.323 devices utilized
- Connect divergent networks by translating between signaling protocols for call setup, teardown, and converting media formats between dissimilar networks, such as Ethernet and ISDN

Notes

Gatekeepers

Without Gatekeepers, each device must be manually configured for inter-device communications. Other characteristics of gatekeepers are:

- Provide a centralized service to which all H.323 devices register
- Perform address translation and bandwidth management on an IP network
- Map LAN aliases to IP address, provide address lookups, and maintain E.164 addresses, when needed
- Exercise call control functions to minimize the number of H.323 connections and the total bandwidth used in an H.323 zone
- Provide accounting, billing, and chargeback capabilities

Table 2: Required Gatekeeper Functions

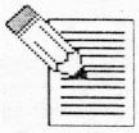
Gatekeeper Function	Description
Address Translation	Provides for translation of alias address, such as URL, to transport address, such as IP; uses registration and update messages to build translation tables
Admissions Control	Provides LAN access authorization, utilizing Admission Request, Confirmation, and Reject (ARQ/ACF/ARJ) messages Access can be based on call authorization, bandwidth, or other criteria; Admissions Control can also be a null function admitting all requests
Bandwidth Control	Supports Bandwidth Request, Confirmation, and Reject (BRQ/BCF/BRJ) messages that can be utilized in bandwidth management; Bandwidth management can also be a null function accepting all bandwidth change requests
Zone Management	Provides above functions for terminals, MCUs, and Gateways registered within its management Zone

Notes

Table 3: Optional Gatekeeper Functions

Gatekeeper Function	Description
Call Control Signaling	Can process Q.931 call control signals in point-to-point conference and can send Q.931 signals directly to endpoints
Call Authorization	Criteria can reject call from a terminal based on Q.931 Rejection can include, but is not limited to, restricted access to/from particular terminals or Gateways or restricted access during certain periods of time Criteria for authorization pass or fail is outside the capability of H.323
Bandwidth Management	If sufficient bandwidth is not available or if a terminal requests additional bandwidth, can reject call Criteria for determining available bandwidth is outside the capability of H.323
Call Management	Maintains a list of ongoing H.323 calls to determine whether a called terminal is busy or to provide information for Bandwidth Management function

Notes



Multipoint Control Units

Characteristics of MCUs are:

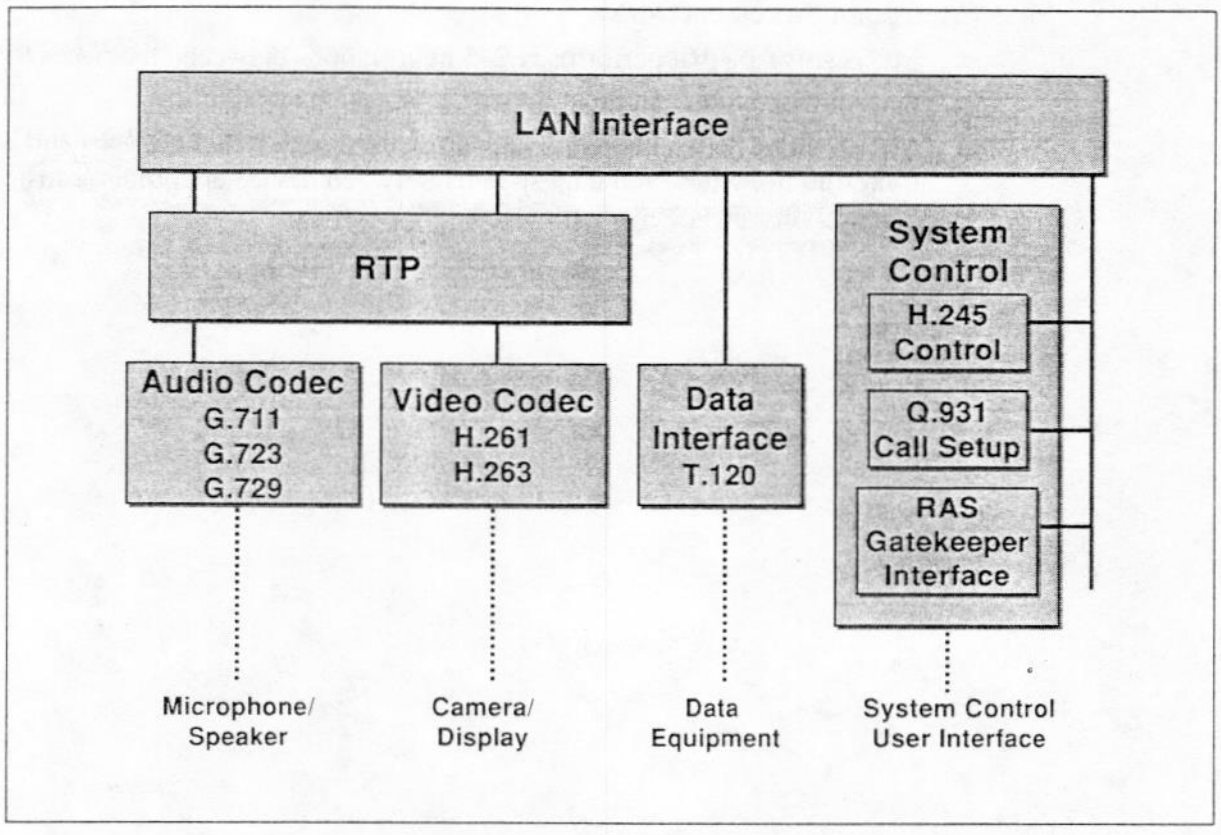
- Support conferences between three or more endpoints
- Consist of a required Multipoint Controller (MC) and zero or more Multipoint Processors (MPs)
  - MC is software that performs H.245 negotiations between all devices to determine common audio and video processing capabilities
  - MP provides both a hardware and software function that encodes and routes audio, video, and data streams between device endpoints; can co-exist on same device with Gatekeeper software

Notes

Terminals

Terminals are considered client endpoints on the network. All terminals must support voice communications. Video and data support is optional.

Figure 5: H.323 Terminal Equipment



Notes

Role of the Multipoint Control Unit

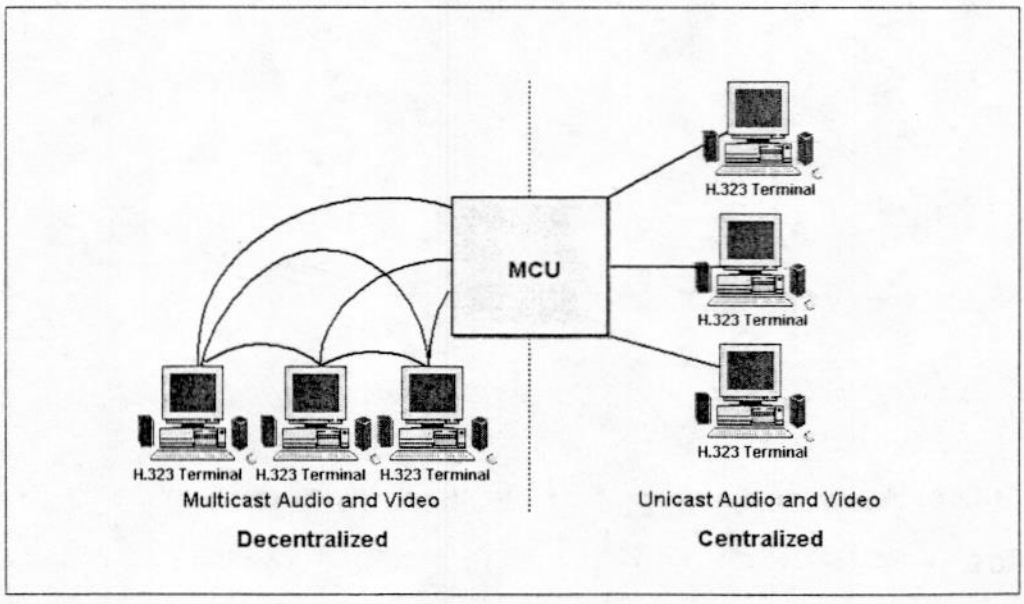
The MCU plays a pivotal role in the establishment of conference calls and the downloading of information to multiple sites. There are two ways this function can be accomplished:

- **Multicast (Decentralized):**
  - Occurs directly from an H.323 device
  - Ensures each device is conforming to standards
  - Uses negotiations conducted by the MC
  - Reduces bandwidth requirements, since all endpoints in the multicast group receive a single data stream
- **Unicast (Centralized):** Uses transcoding or translating protocols of various CODECS and rates, or enforcement of common set of protocols and rates; is provided by centralized MCU

MCU accepts audio stream from the conferees, encodes it into a common signaling format, and regenerates this signal back out to all participants.

Sends multiple point-to-point transmission, yet is considered inefficient, because packets are replicated throughout the network

Figure 6: Multicast and Unicast Conferencing

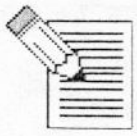


H.323 Protocols

utilizes various protocols to support communications between endpoints, such as terminals, Gateways, and MCUs. These protocols are:

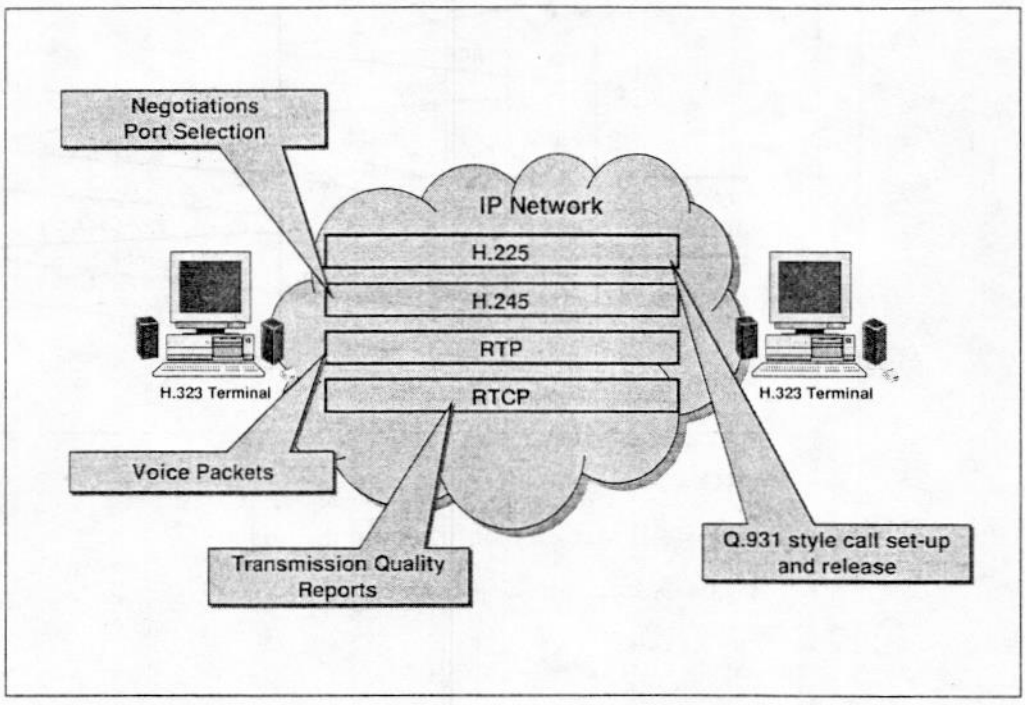
- **H.225:**
  - Establishes the first connection, typically to port 1720
  - Performs registration, admission control, bandwidth changes, status, and disconnect procedures between endpoints and gatekeepers
  - Utilizes the Q.931 signaling method
  - Utilizes Fast Connect or Fast Call Setup, which carries the H.245 signaling information within the H.225 message
- **H.245:**
  - Negotiates audio and video codecs to ensure disagreements are efficiently settled
  - Transmits DTMF codes, lamp indicator control, and other control signaling information required by an H.323 device, in addition to opening and closing media channels
- **H.325:** Used for security

Notes



- **RTP/RTCP:**
  - RTP utilizes User Datagram Protocol (UDP) and provides end-to-end delivery services of real-time audio and video through payload-type identification, sequence numbering, timestamping, and delivery monitoring
  - RTCP provides control services and feedback on the quality of the data distribution, and is intended to typically be utilized as a troubleshooting tool
- **Q.931:** Defines and specifies call signaling and call setup acknowledgements and requirements

Figure 7: H.323 Protocols

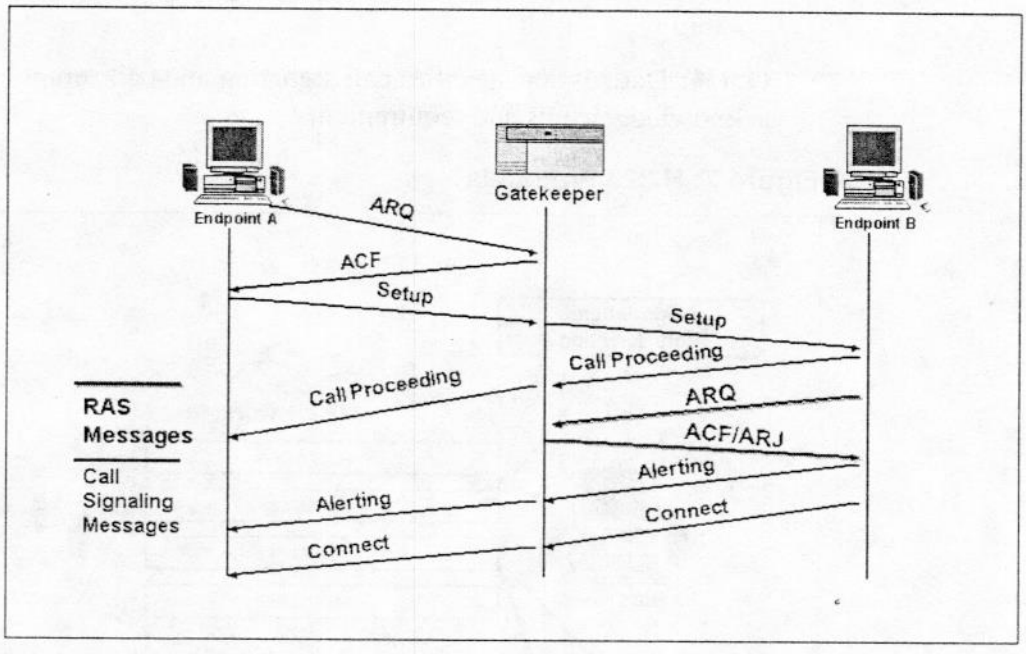


Notes

H.323 Major Operations

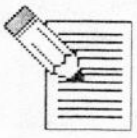
While transporting information, H.323 proceeds in phases from endpoint to endpoint. Different scenarios of call setup can occur, based on whether a Gatekeeper is involved in the communications process. Following is an example of major H.323 phases, which include a Gatekeeper.

Figure 8: Call Setup Operations of H.323



- **ARQ** = Admission Request message
- **ACF** = Admission Confirmation message
- **ARJ** = Admission Reject message

Notes



Explanation of the H.323 Call Setup Operation

Following is a description of the call setup operation:

1. Endpoint A sends the RAS **ARQ** message on the RAS channel to the Gatekeeper for registration. Endpoint A requests the use of direct call signaling

2. Gatekeeper confirms the admission of Endpoint A by sending **ACF** to Endpoint A. Gatekeeper indicates in **ACF** that Endpoint A can use direct call signaling

3. Endpoint A sends an H.225 call signaling **Setup** message to Endpoint B to request a connection

4. Endpoint B responds with H.225 **Call Proceeding** message to Endpoint A

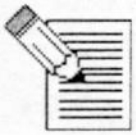
5. Endpoint B has to register with the Gatekeeper and sends an RAS **ARQ** message to the Gatekeeper on the RAS channel

6. Gatekeeper confirms the registration by sending an RAS **ACF** message to Endpoint B

7. Endpoint B alerts Endpoint A of the connection establishment by sending an H.225 **Alerting** message

8. Endpoint B confirms the connection establishment by sending an H.225 **Connect** message to Endpoint A, and the call is established

Notes



Interoperability of H.323

Although H.323 provides a common set of procedures for performing client registration, call setup, call teardowns, and other functions, interoperability issues arise due to the different interpretations of the standard by manufacturers and vendors. This often leads to problems in establishing communications between different manufacturers' equipment in the early stages of development. To ensure vendor and equipment H.323 compliance, interoperability testing is sponsored by International Multimedia Teleconferencing Consortium (IMTC). The mission of IMTC is to assist in the delivery of standards-based and rapid development of conferencing products and services. In addition, IMTC promotes the importance of industry-wide interoperability.

Notes

Well-known Ports

Within networking, port numbers are defined and tend to be reserved for frequently used, higher level processes. Regardless of which customer network or which endpoint, these ports typically remain the same.

Some examples of well-known ports are:

- **25:** SMTP
- **80:** Web
- **110:** POP
- **1718:** Gatekeeper discovery
- **1719:** Registration with the Gatekeeper
- **1720:** H.225 destination

Notes

Session Initiation Protocol

Initially created for the distribution of multimedia content, Session Initiation Protocol (SIP) was designed to be scalable and to utilize existing protocol tools that integrated well with other IP applications, such as email or WWW. Defined by IETF RFC 2543, interoperability is another key goal of SIP.

Key functions of SIP are:

- Supports interactive communications between users
- Handles session initiation, termination, and modification
- Describes session content through the use of Multipurpose Internet Mail Extensions (MIME)
- Determines the location, or presence, of the user within the network
- Supports multicast, unicast, a mesh of unicast sessions, or a combination of unicast and multicast:
  - **Unicast:** Communications only between a single sender and a receiver over a network
  - **Multicast:** Communications between a single sender and multiple receivers
  - **Anycast:** More commonly referred to as a broadcast; Provides communications between a single sender and all devices on the same subnet
- Supports mobile users

Notes

Components of Session Initiation Protocol

Based on a client-server model architecture, SIP components consist of the Server, the Registrar, the User Agent Server, and the User Agent.

Server

The Server accepts request messages from the client and forwards accordingly; sends back responses to the client's requests.

- Proxy Server:
  - Functions as a server and a client in order to make requests on behalf of other clients
  - Supports requests locally or forwards on to other servers
  - Interprets and may rewrite a SIP request message prior to forwarding to another server or to user agent
- Redirect Server:
  - Accepts a SIP request, maps the address in the request to a new address, and returns the appropriate message to the client
  - Does not "forward" SIP requests to other servers and does not accept calls

Registrar

The Registar performs these functions:

- Accepts REGISTER request and is typically co-located with a proxy or redirect server; may offer location services
- Registers SIP parties in a SIP domain that is within the administrative entity for a SIP provider

Notes

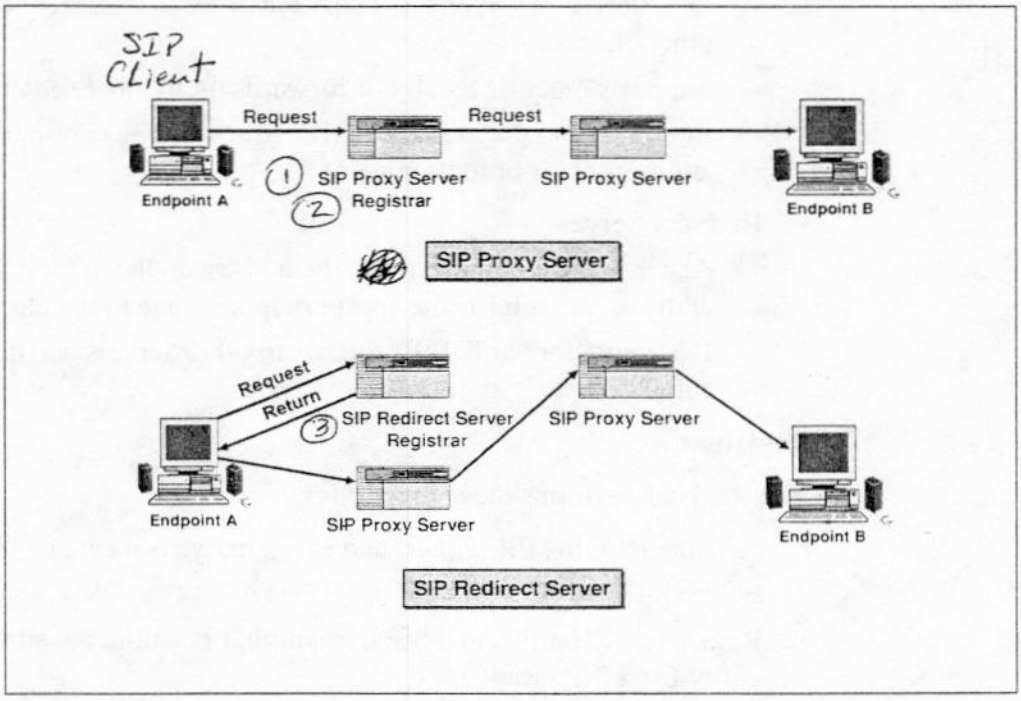
User Agent Server

The User Agent Server (UAS) contacts the user when a SIP request is received and returns an appropriate response on behalf of the user.

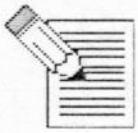
User Agent

The User Agent (UA) contains both a User Agent Client (UAC) and User Agent Server (UAS).

Figure 9: Session Initiation Protocol Architecture Overview



Notes



Session Initiation Protocol

SIP is based on a request-response model or INVITE to a Uniform Resource Locator (URL), or Internet address, for establishment of a session. The protocols that can be utilized to establish a session are: Session Description Protocol (SDP), Session Announcement Protocol (SAP), and Real-Time Streaming Protocol (RTSP).

Session Description Protocol

The SDP performs these functions:

- Conveys setup and media information pertaining to session recipients
- Conveys sufficient information to SIP entities to allow them to join and participate in the session

Session information includes the following:

- Purpose of the session
- Name of session
- Time of the session
- Media type pertaining to the session, such as video and audio
- Formatted information for the video or audio session
- Pertinent IP addresses and port numbers for the session

Session Announcement Protocol

The SAP is an IETF experimental standard. The SAP performs these functions:

- Delivers SDP packets using multicasting where participants are not known in advance; a multicast session is announced by sending multicast packets to a well-known multicast group carrying an SDP description of the session to occur
- Creates, modifies, and terminates sessions
- Contains SDP as payload
- Compares to a television schedule
- Announces a conference session by periodically multicasting an announcement packet to a well known multicast address and port

Real-Time Streaming Protocol

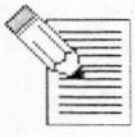
The RTSP supports the control of delivered multimedia stream to include pause, fast forward, reverse, and absolute positioning within the media stream, recording, and device control.

Advantages of Session Initiation Protocol

There are several advantages to SIP that are ideal to a VoIP network. They are:

- **Integration:** Works well with various applications utilizing URLs, supporting MIME, and carrying images, MP3s, and Java applets, in addition to utilizing email routing mechanisms
- **Scalability:** Supports several types of proxy servers
- **Extensibility:** Consists of several mechanisms for extension of protocol
- **Flexibility:**
  - Allows utilization of the protocol, as needed
  - Does not dictate architecture, usage patterns, or deployment scenarios, but rather provides a framework within which it operates
  - Relies on other protocols and techniques to provide QoS
  - May not send INVITE over the same networks that voice packets travel
  - Remains totally independent of the voice path
  - Allows a caller to be routed through an H.323 gateway for processing
- **Mobility:**
  - Supports personal mobility, allowing networks to identify end users regardless of location on the network
  - Allows end users the ability to originate and receive calls and access services on any network device, such as PC, laptop, or IP phone, regardless of location

Notes



Disadvantages of Session Initiation Protocol

In addition to the advantages, there are disadvantages to SIP. They are:

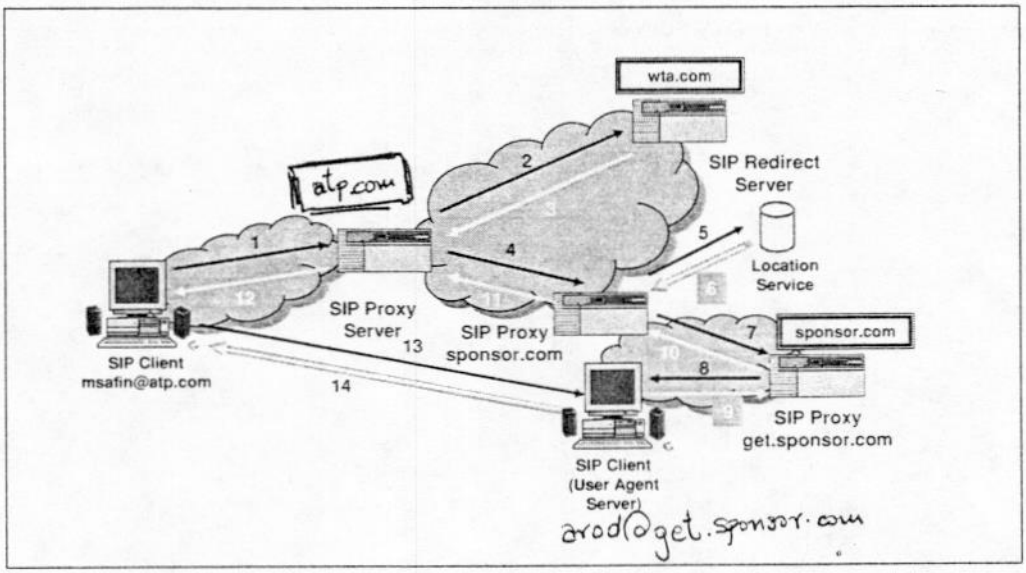
- Increasing shortage of IP v4 numbers
- Growing use of NATs may prevent private Internet endpoint from receiving INVITE
- Transporting media to an address through firewalls can cause removal of information, unless a rule is established to allow media to pass through proxy servers

Notes

Session Initiation Protocol Major Operations

SIP operations follow a different set of procedures when inviting a participant to a session as compared to an H.323 Call Setup. There can be instances when the INVITE has to be redirected and a User Agent located. This is one of the valuable advantages of this protocol. Following is a example of such an INVITE, which has to be redirected to locate an invited participant.

Figure 10: Session Initiation Protocol Major Operations



Use the following information to understand the flow of information.

1.	msafin@atp.com sends a SIP INVITE message to atp.com proxy to place a call to arod@wta.com
2.	atp proxy forwards request to wta.com server
3.	wta server determines arod is temporarily at sponsor.comwta.com server sends redirect to atp.com proxy to try sponsor.com
4.	atp proxy sends INVITE to arod@sponsor.com
5.	sponsor.com server consults its database
6.	sponsor.com determines arod is located at get.sponsor.com
7.	sponsor.com sends new URL to arod@get.sponsor.com and sends INVITE to get.sponsor.com proxy
8.	get.sponsor proxy forwards INVITE to arod's PC after SIP used REGISTER action to ensure location of arod through an address binding procedure; arod responds to request
9-10, 11, 12	response is forwarded back through proxies to original caller
13.	ACK is sent
14.	Session is established and media is transmitted

Session Initiation Protocol Requests and Response Types

Various acknowledgements and responses occur during a SIP Request between User Agents (UA), SIP Proxy Servers, SIP Redirect Servers, Registrars, and User Agent Servers (UAS). It is important to know the SIP Requests, in addition to some of the key SIP Response Types, that occur during the call setup process. SIP Requests are:

- **INVITE**: Starts a session
- **ACK**: Confirms User Agent has received final response to an INVITE
- **BYE**: UA uses BYE to tell server to release the call
- **CANCEL**: Cancels pending request, but not the completed request
- **OPTIONS**: Only requests information about capabilities
- **REGISTER**: Provides user's location to a SIP server

There are a number of SIP Response Types to indicate the progress of a Call Setup. Following are some of the key Response Types:

- 1xx Trying
  - **180** Ringing
- 2xx Successful connection
- 3xx Redirection
  - **305** Use Proxy
- 4xx Request Failure
  - **407** Proxy Authentication Required
  - **415** Unsupported Media Type
  - **483** Too Many Hops
  - **484** Address Incomplete
  - **486** Busy Here
- 5xx Server Failure
  - **502** Bad Gateway
  - **504** Gateway Time-out
  - **505** Version Not Supported
- 6xx Global Failures
  - **600** Busy Everywhere
  - **603** Decline

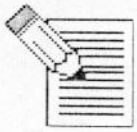
Session Initiation Protocol INVITE

A SIP INVITE is required in order to set up a Media session. The information contained in the INVITE will be different based on the type of Media session, message body length, and various other data. Following is an example of the INVITE sent by msafin@atp.com to arod@wta.com.

Figure 11: Session Initiation Protocol INVITE

INVITE sip: arod@wta.com SIP/2.0	SIP URL of the called party
Via: SIP/2.0/UDP msafin.atp.com	Indicates path taken by the request
From: Marat <sip:msafin@atp.com>	Initiator of request
To: Andy <sip:arod@wta.com>	Recipient of request
Call-ID: 1113244434@atp.com	Uniquely ID's a particular invitation
Cseq: 1 Invite	Command Sequence – Uniquely ID's a request within a Call-ID
Subject: Your tennis game	Nature of the call
Cont-Type: application/SDP	Indicates the Media type in message
V=0	Protocol version
0=Marat 76329381938 IN IP4 192.168.3.2	User, session ID, network type, Address
S=marat203	Session name
C-IN IP4 192.168.3.2	Connection info
M-audio 5004 RTP/AVP 0 12 18	Media name, port address, Codec options available from client

Notes



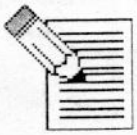
Session Initiation Protocol and Mobility

As stated earlier, an advantage of SIP is the ability to support mobility, whether terminal or personal. Terminal mobility occurs when terminals move between subnetworks supported by Global System for Mobile Communications (GSM) and wireless LAN technology. This technology requires mobile hosts to inform their home proxy servers of their new locations using the REGISTER procedure. In-progress mobile calls also need to inform their home proxy servers of their constantly changing location through the REINVITE procedure.

Current issues regarding mobility are:

- Triangular routing increases delay
- Tunnelling increases bandwidth consumption

Notes



H.323 Versus Session Initiation Protocol

There are distinct differences between the ITU-T H.323 and the IETF SIP, and how they support VoIP. For instance, H.323 specifies a complete, vertically integrated system, while SIP can be built utilizing a variety of architectures and protocols. Following are additional differences between the two protocols:

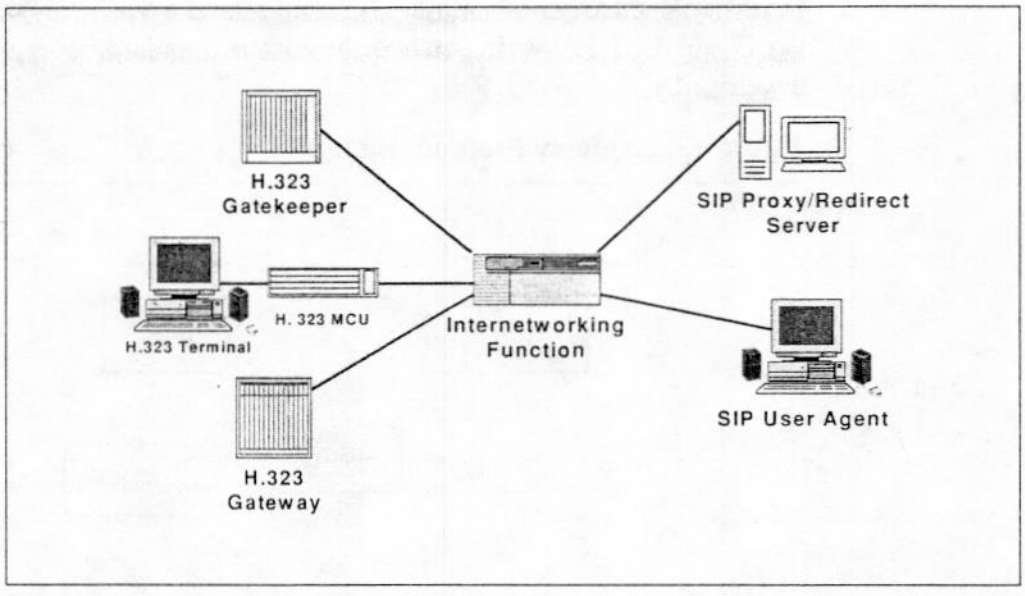
Table 4: H.323 Versus Session Initiation Protocol

Aspect	SIP	H.323
Origin	Networking community (IETF)	Telecom community (ITU)
Architecture	Element	Stack
Encoding	HTTP-like	ASN.1
Network Intelligence and Services	Provided by Servers (Proxy, Redirect, Registrar)	Provided by Gatekeepers
Clients	Intelligent	Intelligent
Emphasis	Multimedia, multicast, telephony	Telephony, video, whiteboard, document sharing
Transport	Mostly UDP	V1=TCP; V2=UDP
Address	SIP URLs	Aliases
Service		
Call Hold	Yes	Yes
Call Transfer	Yes	Yes
Call Forward	Yes	Yes
Call Waiting	Yes	Yes
Third-Party call	Yes	No
Conference	Yes	Yes
Click-to-Dial	Yes	Yes
Capability Exchange	Yes	Yes
QoS		
Call Setup Delay	1.5 rt	2.5 rt
Packet Loss Recovery	Yes	Yes
Loop Detection	Via Hops	Path Value
Fault Tolerance	Yes	Backup

Interworking H.323 and Session Initiation Protocol

Though H.323 and SIP are architecturally different and support many functions differently, they do share some similarities. SIP to H.323 translations and interworking between these two protocols exist. Two functions, such as call setup and teardown, can work between the two. The eventual use of SIP/H.323 gateways will allow deployment of SIP application servers in H.323 networks, providing a migration path towards new services without dismantling their H.323-based network.

Figure 12: H.323 and Session Initiation Protocol Interworking



Notes

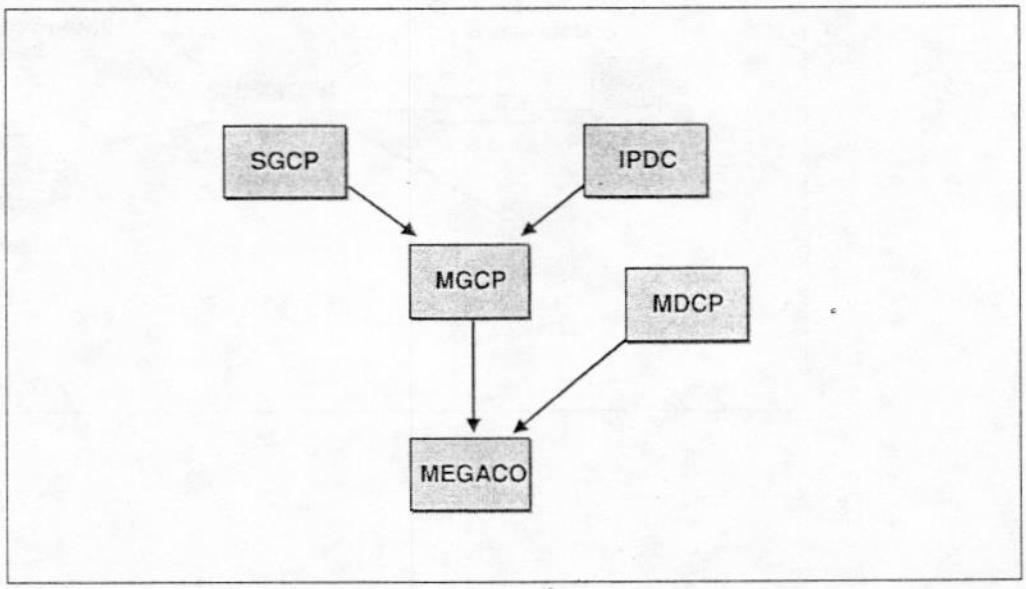
Other Signaling Protocols

There are two relatively low-level device-control protocols that instruct a Media Gateway to merge streams coming from an external cell or packet network onto a cell or packet stream, such as RTP. In addition, these protocols also provide call setup and clear voice or video calls in a packet network, though the tasks they follow are different. These device-control protocols are:

- Media Gateway Control Protocol (MGCP)
- MEGACO/H.248

In reality, due to a combination of resources and agreements between the ITU, ITEF, and the ETSI, MEGACO is the current standard being adopted and developed.

Figure 13: Gateway Protocol History



Notes

Media Gateway Control Protocol

IEFT RFC 2705 defines the scope of MGCP within the IP network. MGCP is actually a merger of the Internet Protocol Device Control (IPDC) and Signal Gateway Control Protocol (SGCP).

IPDC is a suite of protocols that can, individually or together, perform connection control, media control, and signalling transports between the circuit-switched network and the Internet. IPDC was developed by a consortium formed by Level 3 Communications.

SGCP is a UDP-based protocol designed to address the concept of a network that combined voice and data on a single packet-switched IP network operating at a low level. SGCP was developed by Bellcore, now called Telcordia Technologies, and Cisco Systems.

MGCP resembles IETF SIP in its functionality. Both IPDC and SGCP addressed the SS7/VoIP issues offering centralized control of VoIP gateways, remote access concentrators, central office switches, and tandem switches. The functionality is similar to the relationship between the SS7 and the PSTN. The differences between the IPDC and SGCP were a result of differing manufacturers and vendors involved in defining the standards and how they approached the goals each utilized. MGCP supports audio communications.

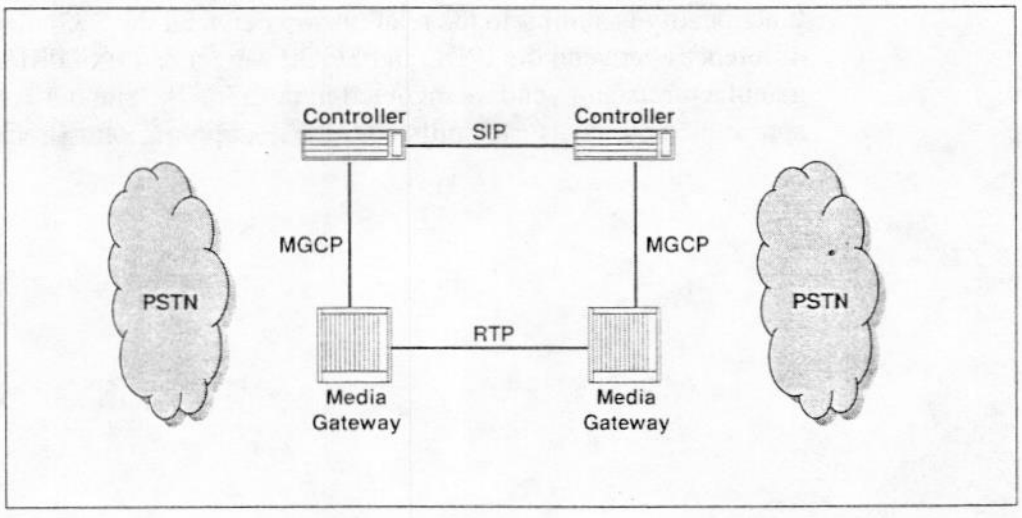
Notes

Role of Media Gateway Control Protocol

The role of MGCP is:

- Decomposes a Telephony Gateway into a controlling signaling component and a controlled media component
- Instructs the controlled media component to send and receive media from specific addresses and to generate tones
- Allows configuration modification
- Ensures the controlled entity reports back to the controller, for instance, when DTMF digits and tones are detected
- Supports an IP phone, with the controller software acting as a PBX to provide features capabilities and call setup through the use of a SIP INVITE to connect the call

Figure 14: Decomposed Gateway



Note: Decomposed Gateway functionally can exist on a single device.

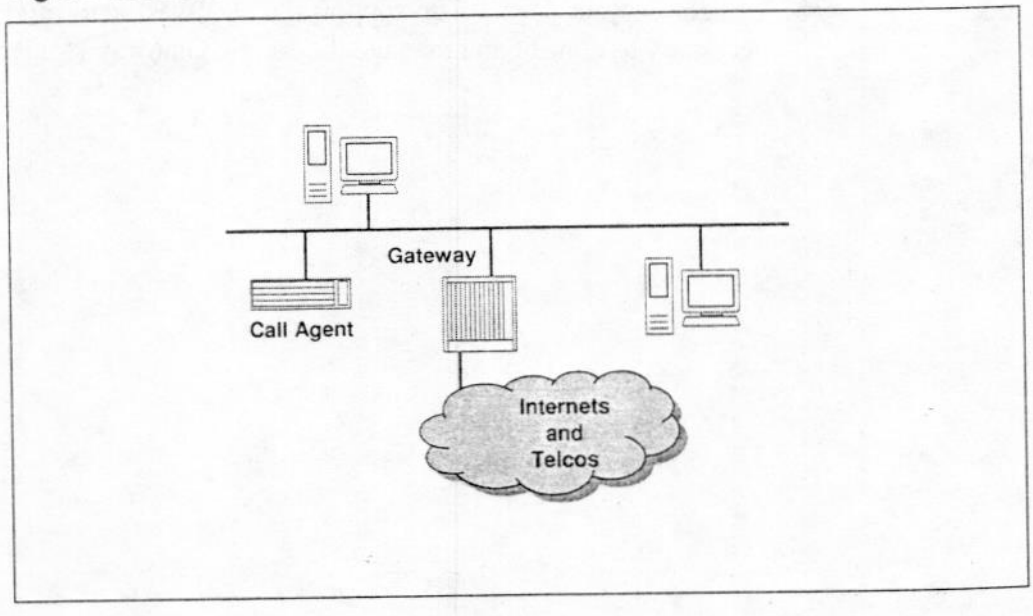
Notes

Components of Media Gateway Control Protocol

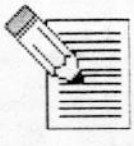
MGCP consists of two key components. They are:

- **Call Agent:**
  - Signalling and call processing, and the Gateway
  - Web-based protocol
  - Software-based program known as a Gateway Controller
- **Gateways:**
  - Network elements that provide audio signal to data packet conversion, which is transmitted on telephony circuitry, the Internet, or other packet networks
  - Endpoint-to-packet network or endpoint-to-endpoint connection in the same gateway

Figure 15: MGCP Architecture Overview



Notes



MEGACO

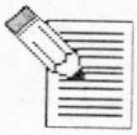
MEGACO is the IETF version of ITU H.248 from the H.323 standards protocol suite, and is the official international standard for decomposed gateway architectures. In addition, MEGACO is the successor to MGCP. Some of the functionalities of MGCP have been incorporated into MEGACO. MEGACO is an ASCII-based protocol and considered similar to HTTP.

H.248, from the H.323 standards protocol suite, also utilizes the ASCII-based protocol, but encodes utilizing the ASN.1 command/response format. MEGACO supports multimedia and has more capabilities for various types of gateways.

MEGACO also supports call processing, using two abstraction concepts for its operations: Terminations and Contexts. These two concepts are used to manage calls and define call states. In addition, MEGACO:

- Allows transactions that consist of several actions and commands
- Provides high availability in the event of equipment or network failures
- Utilizes easy-to-use tools to support the events, signals, and statistics necessary to control and manage the Media Gateway (MG)

Notes

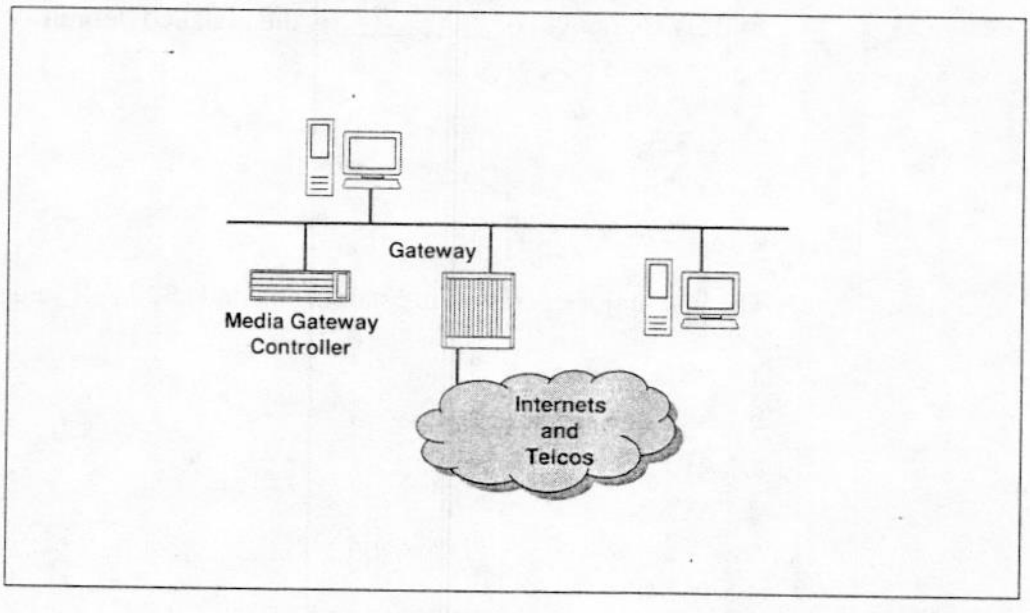


Components of MEGACO

The key to MEGACO and its functionality is the use of its components. They are:

- **Media Gateway Control (MGC):**
  - Provides central point of intelligence for the Media Gateways
  - Controls one or more MGs
  - Communicates to Media Gateway and Signaling Gateway via TCP/IP
- **Media Gateway (MG):**
  - Controls and processes media streams between networks
  - Functions primarily as a slave to execute commands from the MGC
- **Signaling Gateway (SG):**
  - Provides interoperability between the legacy SS7 and the newly-defined Stream Control Transmission Protocol (SCTP)
  - Acts as signaling server created for the PSTN

Figure 16: MEGACO Architecture Overview



Practice

Answer the following questions.

1. Within the H.323 protocol, the standard that defines control parameters is _____.

   a. H.261
   b. G.729
   c. H.225
   d. H.245

2. A key advantage of utilizing H.323 is that H.323 provides a guaranteed QoS.

   a. True
   b. False

3. When programming a codec in an H.323 device for voice transmission on an IP WAN network, _____ is the assigned default.

   a. G.711
   b. G.723.1
   c. G.728
   d. G.729

4. The first major operation in establishing an H.323 call setup is _____.

   a. ARQ
   b. ACF
   c. ARJ
   d. ACK

5. A key function of the SIP Redirect Server is the ability to _____.

   a. Forward SIP requests to other servers
   b. Accept REGISTER requests
   c. Offer location services
   d. Map an address in the request to a new address, returning the message to the client

6. The first major operation in SIP call setup is _____.

   a. DISCOVER
   b. REQUEST
   c. ACK
   d. INVITE

7. A SIP Response Type indicating a successful connection is _____.

   a. 1xx
   b. 2xx
   c. 3xx
   d. 4xx

8. The role of MGCP is to _____.

   a. Decompose a Telephony Gateway into controlling signaling and controlled media components
   b. Provide high availability in the event of equipment failures
   c. Communicate to the MG and SG via TCP/IP
   d. Support Proxy Servers

9. A function of MEGACO MGC is to provide control and intelligence to the MG.

   a. True
   b. False

Answers to Practice

See your instructor for the answers to the Practice.

Notes

Summary

In this lesson, you learned that VoIP standards are determined by organizations attempting to encourage compliance by manufacturers, vendors, and users to ensure a healthy and robust network. In addition, we reviewed the various signaling protocols used by the various manufacturers and vendors in processing information over the IP packet-based network. We also identified the capabilities of interworking between various signaling protocols.

Notes

Notes

Network Assessment

Introduction

To successfully deploy a Voice over IP (VoIP) solution in an existing network, planning is vital. Some key factors to consider are:

- Is the data network ready for VoIP traffic?
- What level of voice quality does the customer expect?
- How will VoIP deployment impact the existing traffic flow?
- What type of VoIP solution is the customer deploying? For example: IP terminals, IP trunks, or both?

Without adequate planning prior to VoIP deployment, the customer can experience poor voice quality, network traffic bottlenecks, or the inability to provide the same level of service to all sites. This can result in customer dissatisfaction and additional time and expense to correct problem conditions.

An effective network assessment is designed to identify potential issues prior to deployment, allowing time to make recommendations and to modify the existing data network infrastructure so the VoIP network meets the customer's expectations and needs.

This lesson guides you through the network assessment process.

Notes

Objective

Given this module and the instructor's presentation, you will be able to complete these tasks:

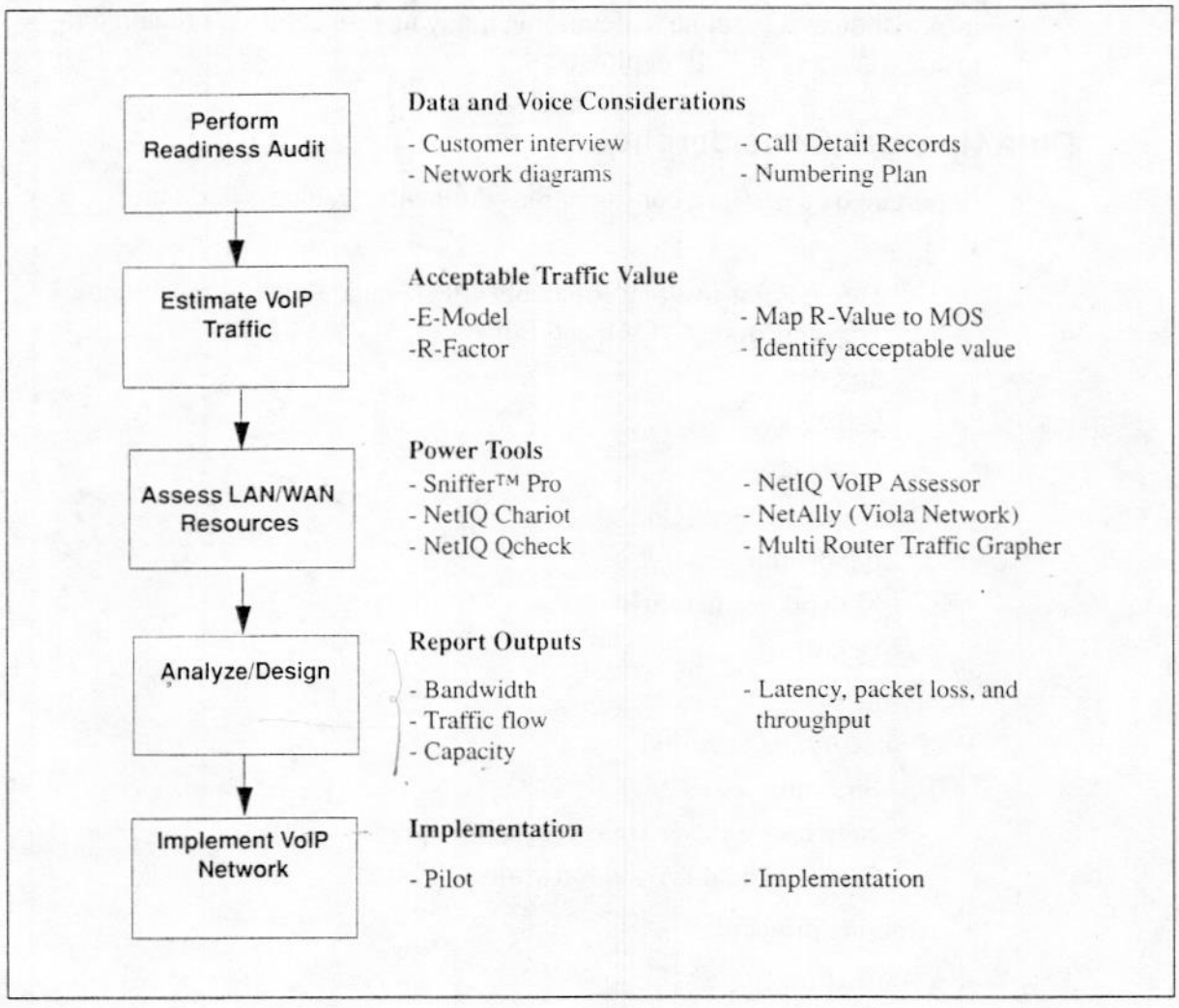
- Define the recommended VoIP network assessment process and areas to prepare for VoIP deployment (such as: link types and speeds, peak delay, packet loss, and LAN/WAN platforms) to prepare for VoIP deployment
- Develop customer recommendations for network improvements based on sample network assessment scenarios in preparation for VoIP deployment
- Identify tools available for use during the network assessment process, such as:
  - Sniffer Pro (sometimes known as Sniffer Portable)
  - Net IQ Chariot
  - NetIQ Qcheck
  - NetIQ VoIP Assessor
  - NetAlly
  - Multi Router Traffic Grapher

Notes

Network Assessment Process Overview

Following is an overview of the network assessment process.

Figure 1: Network Assessment Process Overview



Notes

Perform Readiness Audit

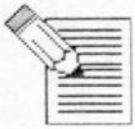
The first step is a readiness audit. During this phase, collect information about the existing data and voice networks. You can obtain this information through customer interviews, diagrams, and system reports. Later, you will use this information as a baseline to determine if any modifications are required to insure a successful VoIP deployment.

Data Network Considerations

Important data network considerations during the readiness audit are:

- Links:
  - Types: Point-to-Point Protocol (PPP), Frame Relay, Asynchronous Transfer Mode (ATM), and Ethernet
  - Speeds
  - Utilization
  - Hardware
- Quality of Service (QoS):
  - Bandwidth
  - Network availability
  - Delay
  - Loss
- Protocols and Security:
  - Firewalls
  - Network Address Translations (NATs)
  - Secure Virtual Private Networks (VPNs)
- Routing protocols
- Traffic flow

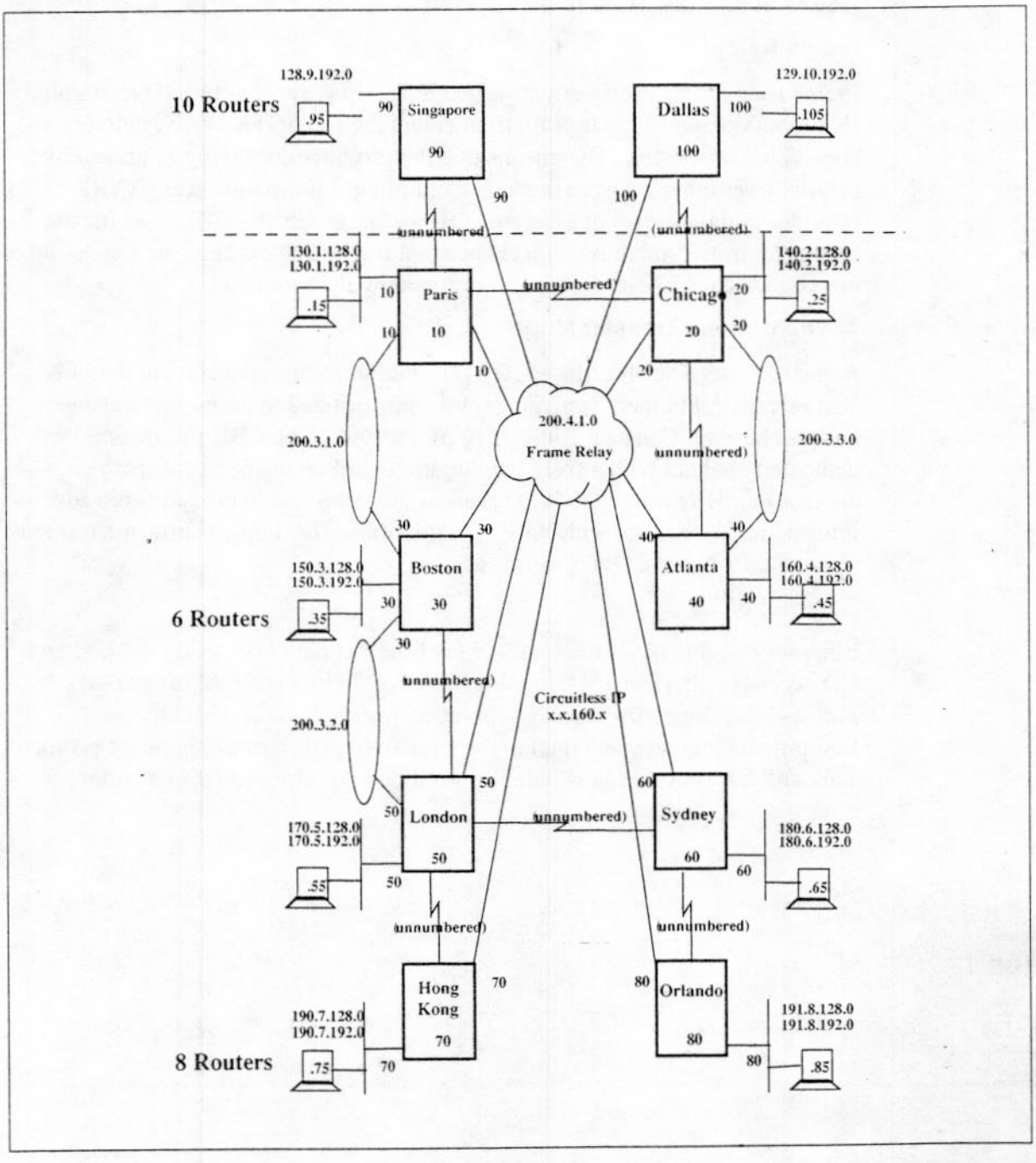
Notes



Network Diagrams

Network diagrams are important to help understand the network infrastructure. For example, connections between devices or sites, addressing, link speeds, and connectivity.

Figure 2: Network Diagram



Link Types

Point-to-Point Links

Serial Point-to-Point links use Point-to-Point Protocol (PPP) to transport data between two hosts over a dedicated link. PPP links provide the most control for QoS, as they are direct point-to-point links and provide dedicated bandwidth. However, they can be more costly.

Frame Relay

Frame Relay is more cost effective than PPP. However, it is based on a publicly shared model. Once the transmission enters the provider's WAN, delivery is considered best-effort. This means that the provider does not guarantee any priority over other transmissions. A Committed Information Rate (CIR) provides a higher level of assurance. However, unless the CIR is set for the total peak traffic, there is still a chance that traffic that exceeds the CIR will be marked Discard Eligible (DE) and dropped by the provider.

Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is similar to Frame Relay, in that it is cost effective, but there is no guarantee of prioritization unless the customer has purchased a Constant Bit Rate (CBR) service. The CBR provides a dedicated channel with a fixed bandwidth, based on the needs of the application. However, with ATM there is an additional overhead for header information associated with VoIP transmissions. This impacts how the frame is segmented and the CODEC used.

Ethernet 802.3

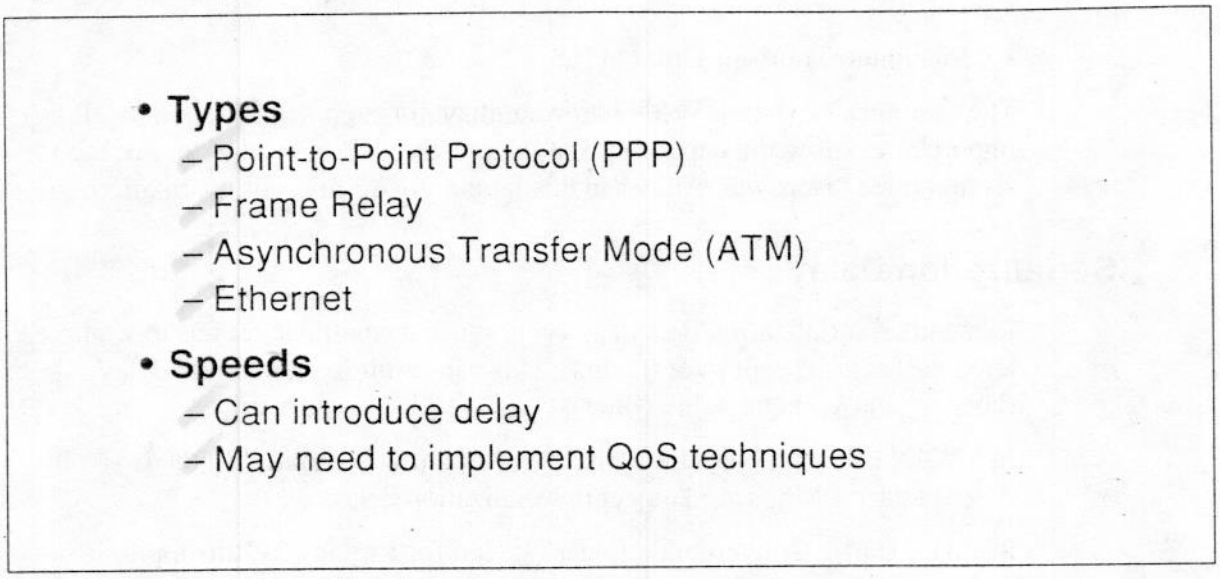
Ethernet 802.3 is the IEEE standard for Ethernet networks using the CSMA/CD access method on a bus topology LAN. Ethernet is a LAN transport protocol developed by Xerox Corporation in cooperation with Digital Equipment Company and Intel in the late 1970s. Ethernet is a network protocol standard that specifies how data is placed on and retrieved from a common transmission medium.

Notes

Link Types and Speeds

Remember, it is important to know the link types used because this impacts the overhead of the packet. In addition to link types, speed is important because it can introduce delay.

Figure 3: Link Types and Speeds



Notes

Implement Quality of Service

It may be necessary to implement QoS techniques, such as:

- Protocol prioritization
- Traffic shaping (for Frame Relay)
- DiffServ
- Maximum Transmit Unit (MTU)

The customer's existing WAN hardware may not support these options. It is important to know the capabilities of the existing WAN hardware. See the section titled "Hardware," later in this lesson, for additional information.

Serialization Delay

Remember, serialization delay can occur when a small packet has to wait for a large packet to be sent over the link. This can result in end-to-end delay (latency) and variable delay (jitter).

In a WAN environment where link speeds are low compared to the LAN, link speeds under 1 Mbps are subject to serialization delay.

See the "Traffic Convergence Issues" lesson for a review of this topic.

Notes

Hardware

The customer's existing LAN and WAN hardware may not support the technologies available to implement QoS in the VoIP network. It is important to know the capabilities of the existing LAN and WAN hardware.

It may be necessary to upgrade, replace, or expand the customer's existing LAN and WAN hardware to meet the performance, redundancy, or QoS functionality requirements of the underlying data infrastructure for the support of VoIP.

When you analyze network devices, especially WAN edge routers, remember that an upgrade of interfaces or link speeds does not always ensure that performance requirements will be met. Although a network router or switch can physically support a T1 or 100 Mb interface, the device may not be able to achieve full throughput on these interfaces. CPU utilizations, device architectures, and activation of traffic filters or access lists can significantly impact performance.

Redundancy

You must also consider redundancy at various levels, such as:

- Interfaces for critical connections,
- Single points of failure in network devices at critical points within the network
- Power
- Whether the combination of the network design and devices provides for redundant or alternate paths in the event of a major link or device failure

Dynamic Host Configuration Server

If a customer plans to deploy soft IP clients, a Dynamic Host Configuration Server (DHCP) might be necessary to deploy soft IP clients on the company's laptops.

Notes

Quality of Service

A converged network mixes different types of traffic, each with very different requirements. These traffic types often react unfavorably when mixed. For example, a voice application expects no packet loss, and a minimal, fixed amount of packet delay. It operates in a steady fashion, with voice packets transmitted at fixed time intervals. This level of performance is obtained on a circuit-switched network.

A best-effort IP network has varying amounts of packet loss, and variable delay usually caused by network congestion, which are the opposite of what is needed by a voice application. This can result in speech distortion, delay, and packet loss.

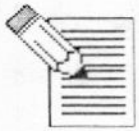
Some important QoS parameters to analyze include: network availability, bandwidth, delay, and loss. As discussed earlier in this lesson in the section titled "Hardware," knowledge of actual device support is essential. See the "Packet Design" and "Traffic Convergence Issues" lessons, covered earlier in this course, for detailed information about QoS options and VoIP traffic requirements for network performance.

Network Availability

Network availability has the most significant effect on QoS. If the network is unavailable, even for brief periods of time, the user or application can achieve unpredictable or undesirable performance levels. Network availability is dependent on the availability of a redundant network. A redundant network generally includes the following elements:

- Redundant devices such as interfaces, processor cards, and power supplies
- Resilient networking protocols
- Multiple physical connections, such as copper or fiber
- Backup power sources

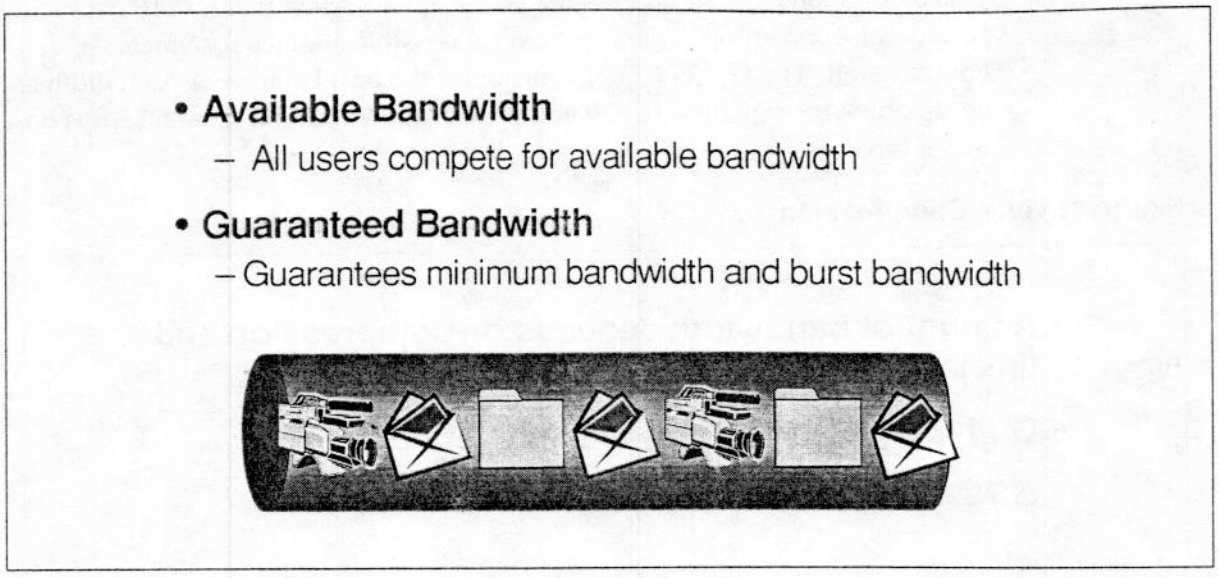
Notes



Bandwidth

Bandwidth is a significant parameter that affects QoS. There are two types of bandwidth: Available Bandwidth and Guaranteed Bandwidth.

Figure 4: Bandwidth



Available Bandwidth

With available bandwidth, the service purchased is typically available, but not guaranteed. For example, a customer purchase 256 Kbps. During light network traffic times, a user can achieve 256 Kbps, but under heavy network traffic conditions, the bandwidth is not achieved consistently. Many network operators oversubscribe the bandwidth on their network to maximize the return on their network infrastructure or leased bandwidth. This still does not ensure consistent bandwidth, as all users compete for available bandwidth.

Guaranteed Bandwidth

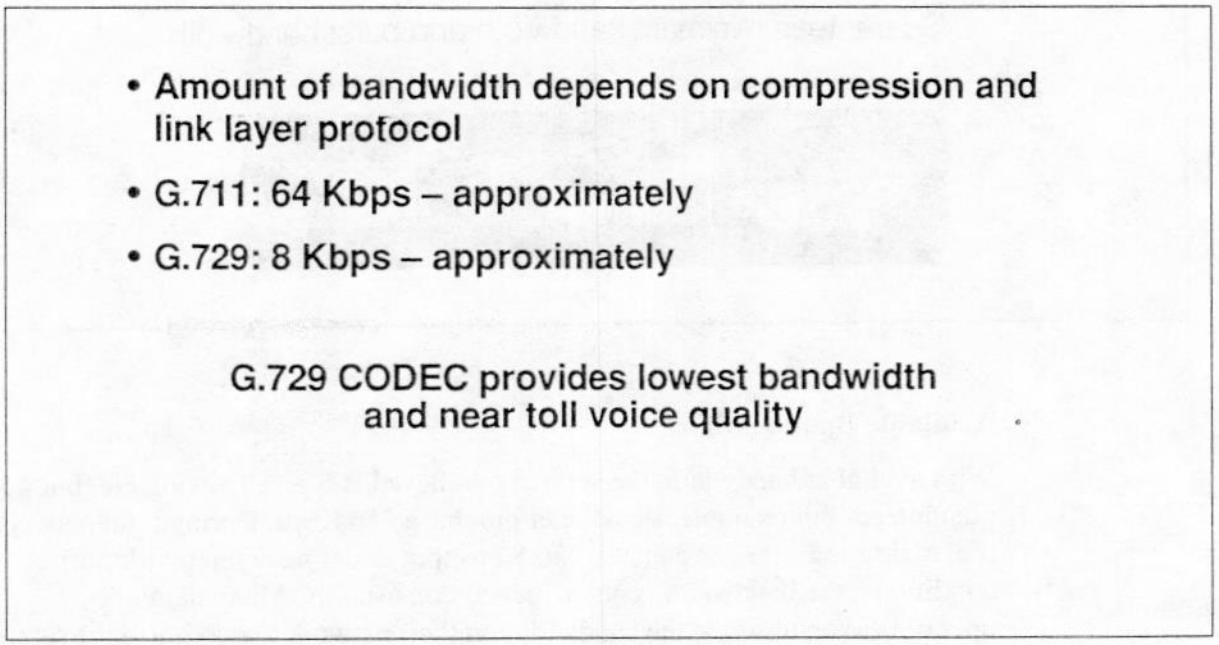
Some providers offer a Guaranteed Bandwidth service that guarantees a minimum bandwidth and burst bandwidth (duration of excess bandwidth use). With Guaranteed Bandwidth, subscribers get preferential treatment (QoS bandwidth guarantee) over the Available Bandwidth subscribers.

Voice Compression

Another consideration with bandwidth is voice compression. The amount of bandwidth used by a VoIP call depends on if the voice signal is compressed and what link layer protocol the VoIP packet uses for transport.

Is is recommended to compress the voice signals when using VoIP over a low bandwidth connection. There are several possible choices for voice compression. The G.729 CODEC provides the best balance of bandwidth and acceptable voice quality. G.729 compresses the voice call from 64 Kbps down to 8 Kbps.

Figure 1: Voice Compression



Note: Bandwidth requirements are estimates.

Notes

Quality of Service Versus Bandwidth

One theory says that QoS is unnecessary. This theory contends that increasing bandwidth provides enough QoS for all applications. This theory also states that implementing QoS is complicated; adding bandwidth is easy. However, it is necessary to look at the QoS problem to determine if adding bandwidth will solve the problem.

If all networks had so much bandwidth available that network congestion never occurred, QoS technology would not be needed. Some carrier network sections have huge amounts of bandwidth that have been carefully engineered to minimize congestion. Some carriers offer low latency connections across their Metropolitan Area Networks (MANs), cross-country networks, and continental long-haul networks.

But high bandwidth connections are not available throughout the entire network. This is especially true for access networks, where the usual amount of bandwidth available is only several hundred Kbps. Traffic must be treated consistently to achieve a prescribed QoS level. Bandwidth differences in a network become potential congestion points. This can create poor quality and unpredictable QoS, even though the long-haul network offers excellent QoS performance.

Notes

Packet Loss and End-to-End Delay (Latency)

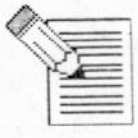
Loss can occur due to errors created by the physical medium used to transmit the data. Loss also occurs when congested network nodes drop packets.

End-to-end delay (latency) is the total time elapsed from speaking into a transmitter at one end to hearing the reconstructed sound on a receiver at the other end. Delay has a significant impact on the quality of a voice call. Most listeners can detect delay greater than 100 milliseconds (ms). At the 150 ms level, the delay becomes annoying.

Variable Delay (Jitter)

Jitter (also known as delay variation) has a pronounced effect on real-time, delay-sensitive applications, such as video and voice. These applications need to receive packets at a fairly constant rate, with a fixed delay between consecutive packets. If the arrival rate varies, the jitter affects the application's performance. Minimal jitter is sometimes acceptable, but if jitter increases, the application can become unusable.

Notes



Protocols

When assessing the network for VoIP readiness, observe the distribution of protocols in the network; specifically, on the WAN. Network Management Systems can poll network devices and analyze the results.

Mixing Protocols

Even with Maximum Transmission Unit (MTU) implemented, if there are protocols in use other than IP, those protocols can maintain larger frame sizes. This can introduce additional delay to the VoIP traffic.

It is important to be aware that certain applications running over IP can set the frames with the "may fragment" bit set to 1, which prevents fragmentation. As part of the overall assessment process, the network analysis on the LAN will determine if there are any applications that have this bit setting.

Time-Sensitive Protocols

Some data protocols such as Structured Query Language (SQL), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP), use primarily unicast traffic. Unicast traffic is traffic that goes to only one machine. This can effect your voice traffic by filling the pipe. Prioritizing the voice traffic should help eliminate this issue. Other chatty protocols such as NetBios Enhanced User Interface (NetBUI) spend much of their time broadcasting information to the network. Broadcasting is a way of sending traffic to all the machines on the network. When a host sees a broadcast message it must take time to read the message. This can interfere with the time sensitive VoIP traffic. Just placing the voice traffic in a higher queue does not avoid this problem since it is actually causing the host (IP terminal or client) to take the time to read the incoming broadcast traffic. If there is a lot of broadcast traffic on the network it is necessary to separate the voice traffic from the data traffic by placing them in separate VLANs. This means the devices on the voice VLAN will not see the traffic from the data VLAN.

Notes

Packet Loss Concealment

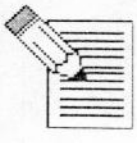
Some network protocols, such as TCP/IP, retransmit dropped traffic. This is a problem for voice calls. Voice calls can not make use of the retransmitted packets because of the delay. When there are gaps in the voice signal due to network packet loss, the quality of the VoIP call will become choppy. In addition, if the traffic was originally dropped because of network congestion, the retransmission causes the congestion to spiral. This is why speech is not sent over a protocol with built in retransmission. It is sent over UDP/IP, which does not retransmit dropped packets.

Packet Loss Concealment (PLC) generates a synthetic replacement signal based on the last signal received. The algorithm changes as more packets are lost.

The G.729 and G.723.1 CODECs have built-in PLC and their quality drops slowly with increasing amounts of packet loss. G.711 and G.726 have no component PLC algorithm, but an external one can be added when these CODECs are used in a packet environment. A T1 standard has been adopted defining the PLC to be used with G.711.5 There is no comparable standard for G.726.

Note: When good packets are restored, G.711 recovers immediately, whereas G.726 (ADPCM) and CELP based CODECs require a short time to re-adapt.

Notes



Security

A good network design considers security. Firewalls and intrusion detection systems protect the enterprise network from outside intrusions. Network address translation (NAT) devices can keep computer addresses hidden from hackers. However, be careful where you place the NAT devices, because it is difficult, if not impossible, to make VoIP work across a NAT.

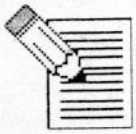
The following security features must be considered:

- Encapsulation of VoIP packets
- Firewall or Network Address Translation (NAT) that natively support H.323 or Session Initiation Protocol (SIP)
- H.323- or SIP-enabled proxy server, used in conjunction with a firewall

Routers might use NAT and IPSec for remote network users who connect to the network through the public internet using IPSec encryption. A firewall connection can be in place, as well.

The network designer must consider the security policy in force, and see if the ports required for VoIP can go through the firewall.

Notes



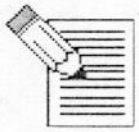
Power and Wiring

Inspect the power and wiring. Additional power or wiring may be necessary to support VoIP devices. For example:

- Power over LAN (sometimes called inline power) for IP terminals
- Redundant power supplies for the network equipment
- Uninterruptible Power Supply (UPS)
- Sufficient cooling in wiring closets for the UPS

Note: If you have redundant power supplies, plug each power supply into a separate UPS. If possible, have each UPS on its own circuit so that if one circuit goes down you still have power from the other circuit.

Notes



Routing Protocols

WAN Protocols

Routing protocols in the WAN can be very important when considering how VoIP calls will be routed and how quickly fail-over occurs. When planning a VoIP network, be aware of what situations trigger a routing table update with respect to the routing protocol. This helps when predicting what path a VoIP flow might take during a failure in the network.

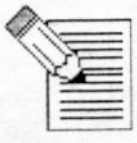
Convergence

Convergence is the point where all internetworking devices have a common understanding of the routing topology. The time it takes a network to re-converge after a link failure must be considered. The process can take several minutes, depending on the network size and routing protocol in use.

LAN Protocols

Routing protocols in the LAN must also be considered when implementing VoIP.

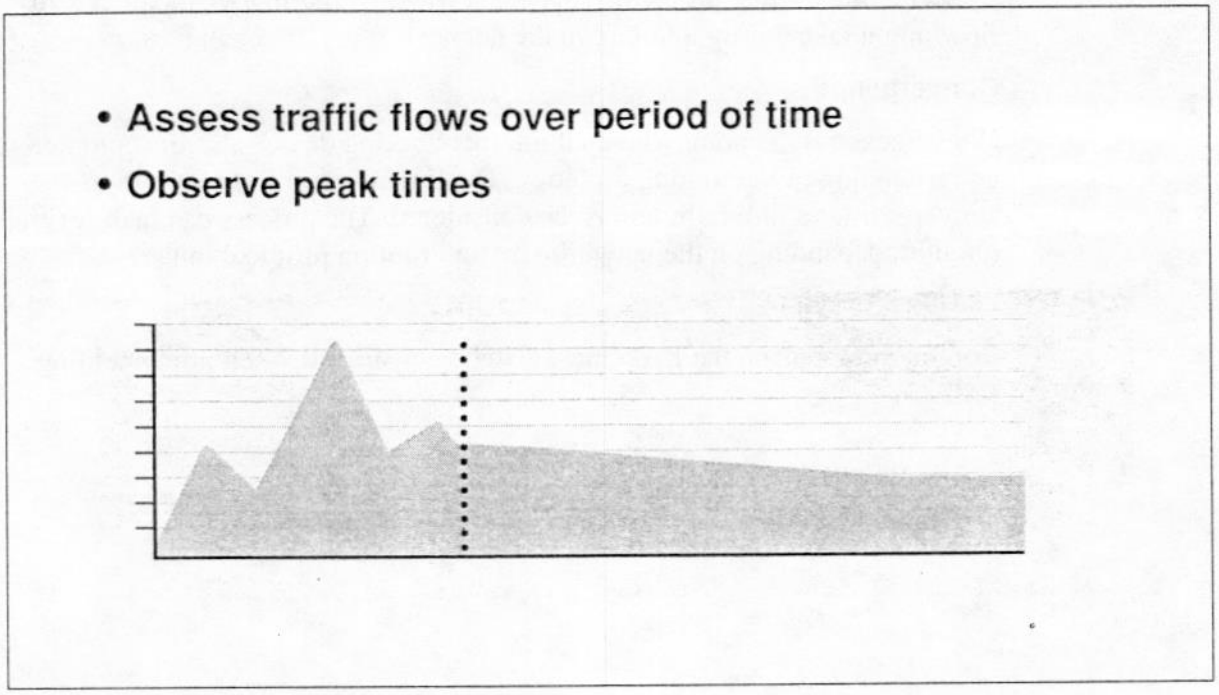
Notes



Traffic Flow

It is important to assess traffic flows over a period of time (a week or longer) depending on the complexity of the network. Observe the peak times of day, week, and month to determine where the highest utilization exists.

Figure 2: Traffic Flow



Notes

Voice Considerations

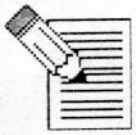
Voice Traffic

From a voice perspective, an understanding of the circuit-switched facilities is important. Some important voice considerations include:

- Flow
- Calling patterns
- Number of users
- Peak values for time of day, day of week, or month

Note: Call Detail Records (CDR) are a helpful resource when analyzing the voice traffic.

Notes



Voice Quality

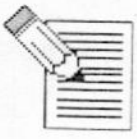
You must also consider a method to ensure that the network consistently provides the same level of quality as the PSTN. Earlier in this course, you learned about some methods to measure voice quality:

- MOS (Mean Opinion Score)
- E-Model (ITU G.107)

The tables on the next page provide additional information about user satisfaction levels, as well as the impact of CODEC on voice quality.

Tip: *It is recommended to use the E-Model, rather than the MOS (Mean Opinion Score), to calculate voice quality. The MOS is not as accurate when applied to VoIP networks, as it assumes the network is circuit-switched.*

Notes



MOS Subjective measure

Assess Network Resources

Once you complete the pre-assessment, you are ready to perform the actual network assessment. An effective network assessment includes the following:

- Simulate VoIP traffic flow
- Assess link utilization
- Observe routing protocols
- Calculate voice quality
- Identify jitter, one-way delay, and packet loss
- Generate detailed reports

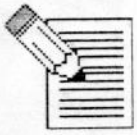
The data and reports generated during the network assessment will help you make recommendations on any modifications that may be required to insure a successful VoIP deployment.

Network Assessment Tools

A variety of software tools are available to help you perform a network assessment. Some these include:

- Sniffer Pro or Portable (Sniffer Technologies)
- NetIQ Chariot (NetIQ Corporation)
- NetIQ Qcheck (NetIQ Corporation)
- NetIQ VoIP Assessor (NetIQ Corporation)
- NetAlly (Viola Networks)
- Multi-Router Traffic Grapher (Swiss Federal Institution)

Notes



Sniffer Portable

Sniffer Portable (also known as Sniffer Pro) is best-suited for identifying the existing protocols in a customer's network to understand if potential problems may arise between applications and QoS recommendations.

This software tool displays network activities on the monitoring PC in colorful graphs and charts. For example:

- Bandwidth utilization
- Packets per second
- Broadcasts and multicasts
- Protocol analysis

Built-in expert network analysis helps you quickly identify faults and troubleshoot outages quickly.

Using the product's reporting tool, you can export data into popular third-party applications to create customized reports.

The figure on the next page is an example of a Sniffer Portable screen.

Notes

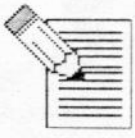
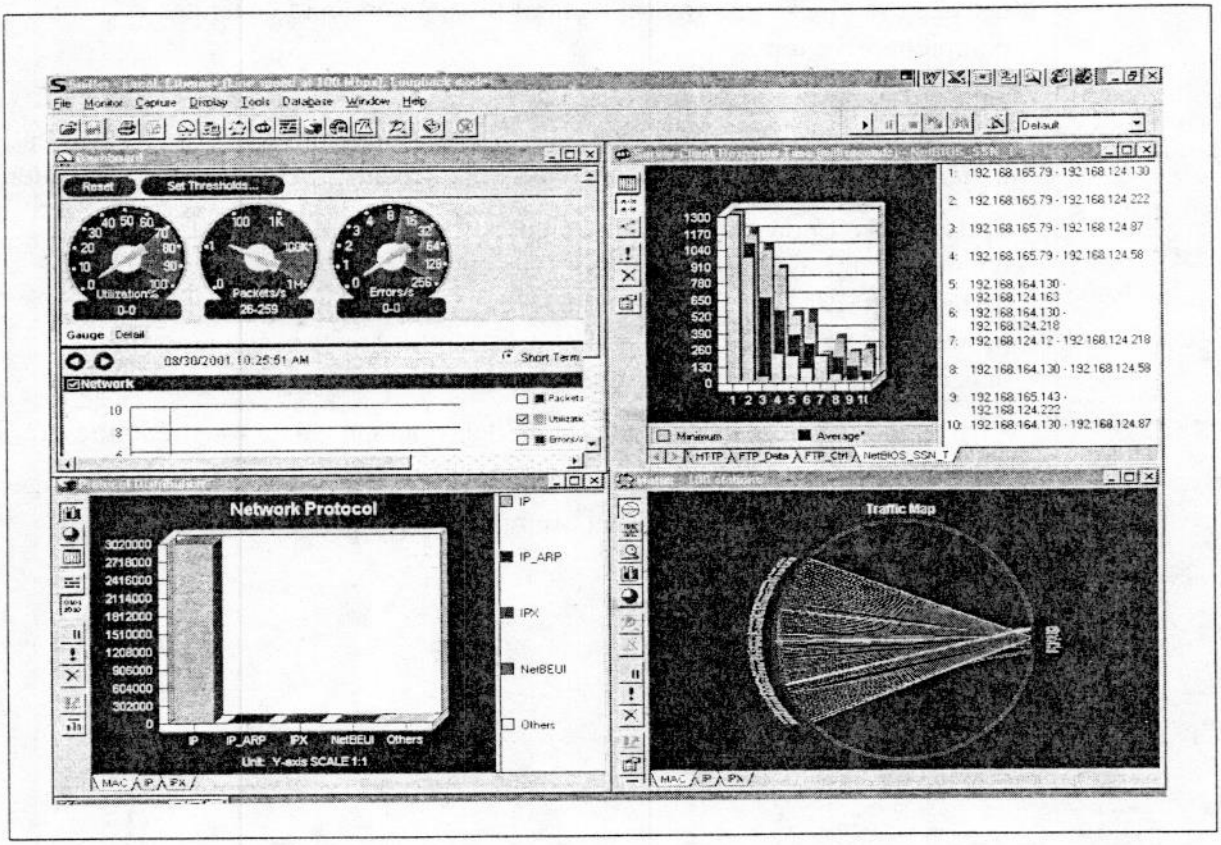


Figure 3: Real-Time Network Analysis



Notes

NetIQ Chariot

NetIQ Chariot (Chariot) emulates transaction traffic from real applications, tests and troubleshoots any segment of the network, and generates comprehensive reports.

Chariot supports a variety of tests that enable you to measure network performance and stress. For example, Chariot's maximum jitter measurement is most significant for identifying QoS impairments, such as latency and jitter.

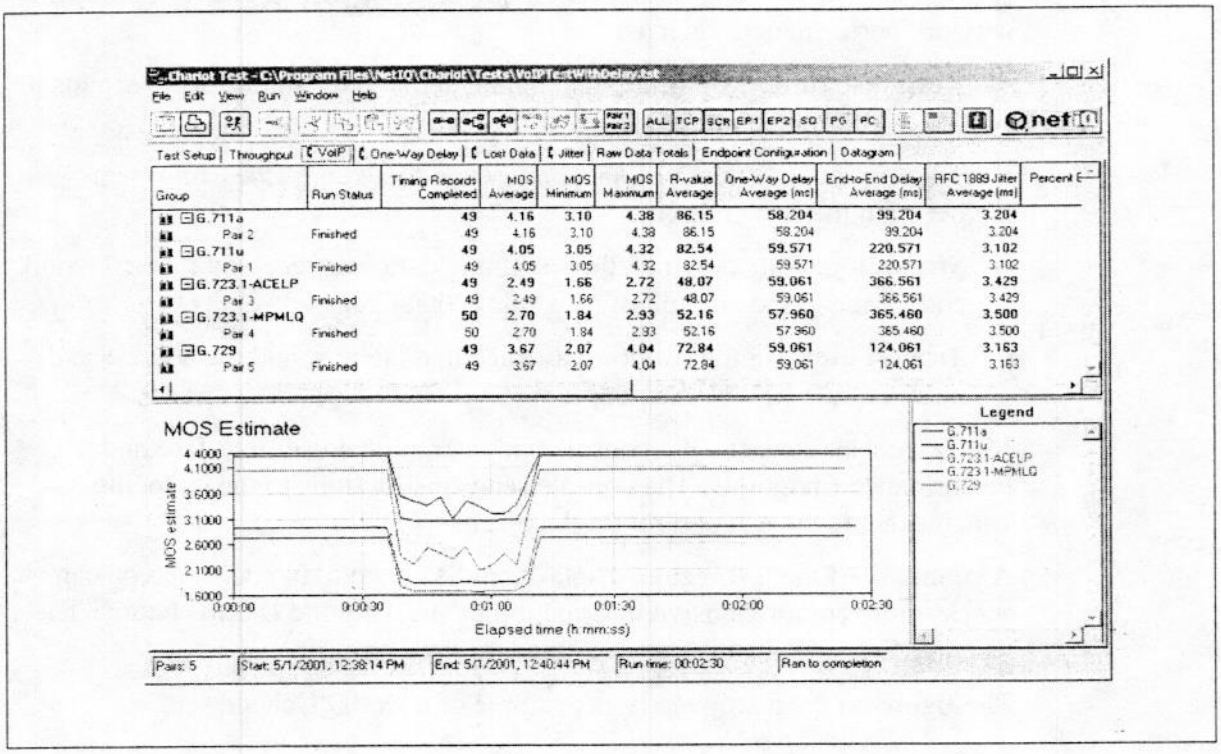
Performance Endpoints, or lightweight software agents, are installed on computers throughout the network. The endpoints emulate network traffic, including traffic with multiple data types, variable data rates, and multiple protocols. The endpoints collect information for analysis and reporting and generate reports that measure end-to-end performance and response time.

Chariot also measures maximum jitter, delay, and lost data for streaming applications.

The figure on the next page is an example of a Chariot screen.

Notes

Figure 4: Chariot VoIP Test Module



Notes

NetIQ Qcheck

NetIQ Qcheck, by NetIQ Corporation, is a free software tool that measures network performance, such as:

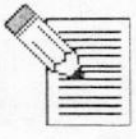
- **Response time:** Minimum, maximum, and average number of seconds it took to complete a transaction
- **Throughput:** Amount of data per second that was successfully sent between the two endpoints
- **Streaming:** Rate at which the streaming data was received by the second endpoint and the amount of packet loss that occurred
- **Traceroute:** Number of hops, average hop latency, and the address and names of the host at each hop

NetIQ Qcheck consists of a console with a graphical user interface and Performance Endpoints. The console sends instructions to the endpoints, which execute the test and return the results.

A summary of the test results displays on the console. In addition, you can access more comprehensive information by pressing the **Details** button. The formatted test results display in a standard Web browser.

The figure on the next page is an example of a NetIQ Qcheck screen.

Notes



NetIQ VoIP Assessor

NetIQ VoIP Assessor (VoIP Assessor) is based on the technology of NetIQ Chariot. VoIP Assessor enables you to predict how well VoIP will work on the network prior to deployment.

VoIP Assessor simulates VoIP traffic and produces reports that help you identify areas of concern, including jitter.

A VoIP Assessor session includes these phases:

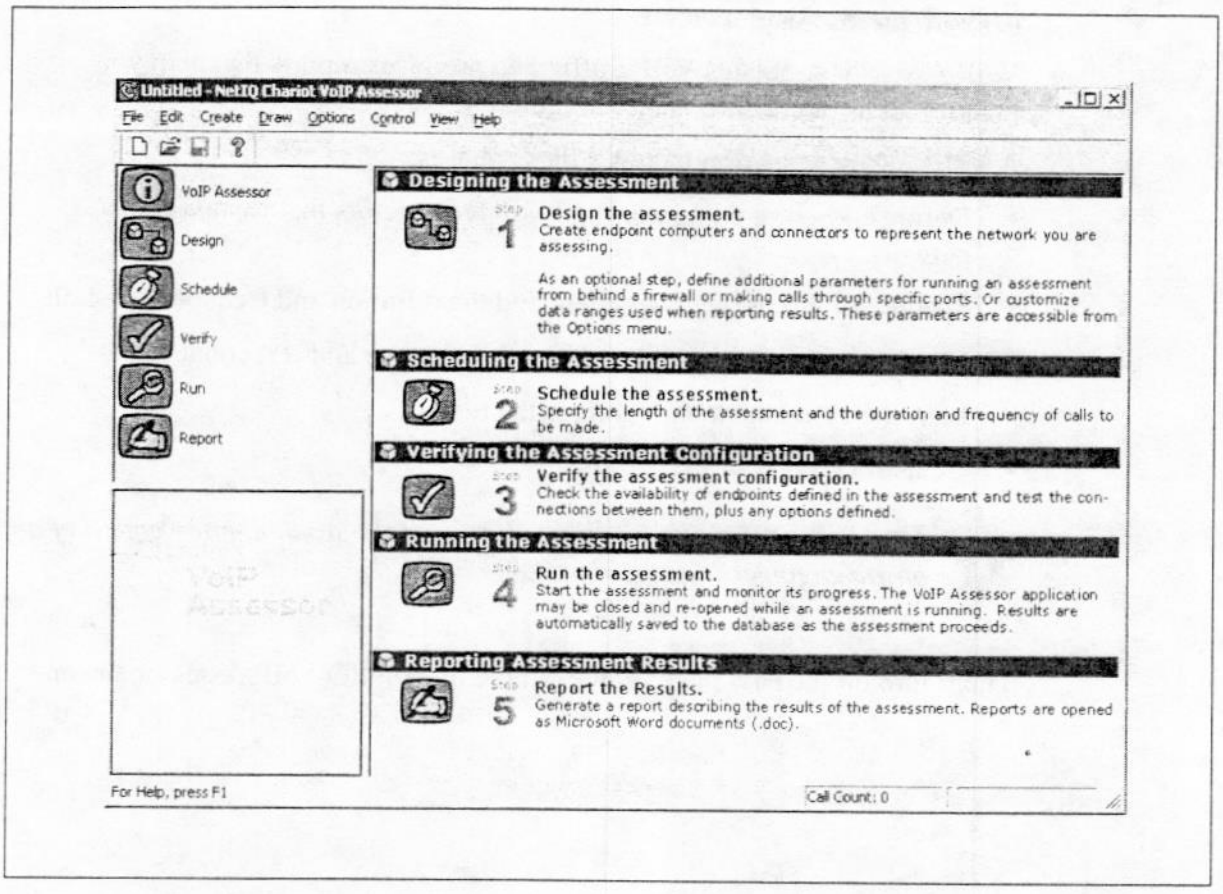
- Define end-point computers and VoIP connectors that represent the network
- Specify length of the assessment and the duration and frequency of calls
- Check the availability of the defined endpoints and test connections
- Start the assessment and monitor the results
- Generate reports of the results

Tip: *Because you specify the duration of the session, intervention of an onsite engineer is not required.*

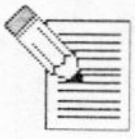
The figure on the next page is an example of a NetIQ VoIP Assessor screen.

Notes

Figure 5: VoIP Assessor Main Menu



Notes



NetAlly

NetAlly (Viola Network) emulates network traffic (as deployed or as planned), analyzes the results, and generates reports at scheduled times or on demand. The primary measurements used in the analysis are delay, loss, jitter, and throughput.

NetAlly consists of a Test Center, which is installed as a management process on a supported server, and Traffic Agents, which are software components that are installed on existing servers or computers at strategic locations within the network. This enables you to rapidly isolate the sources of network performance issues, from the server to the end-user desktop. NetAlly also provides the flexibility to verify the test results by repeating identical tests, as needed.

The figure on the next page is an example of a NetAlly Assessor screen.

Notes

Multi Router Traffic Grapher

The Multi Router Traffic Grapher (MRTG) is an SNMP tool that monitors the traffic load on network links in real time and displays the results on an HTML page.

As a pre-deployment tool, MRTG can determine router and link utilization in a WAN environment. MRTG can collect statistics on any device that has an SNMP agent, and gathers statistics for the day, week, month, and year, without the necessity of an onsite engineer.

In addition to monitoring traffic, you can use MRTG to monitor any SNMP variable you choose; for example: system load, login sessions, and modem availability.

The figure on the next page is an example of an MRTG screen.

Notes

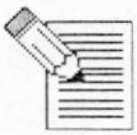
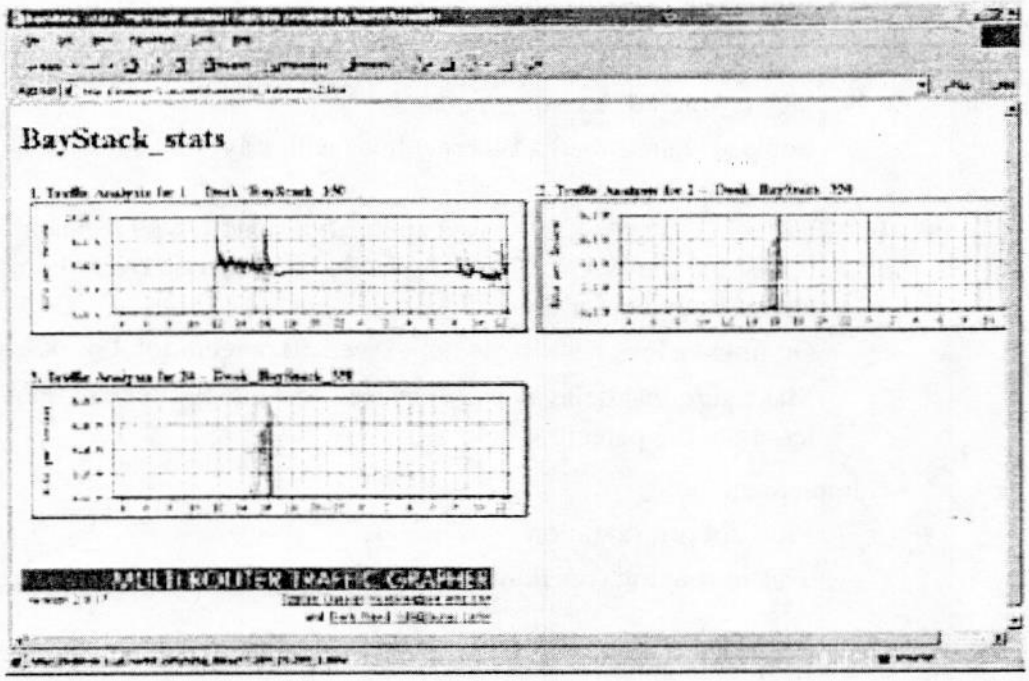


Figure 6: Multi Router Traffic Grapher



Notes

Network Improvements

Once the network assessment is complete, use the information collected during the pre-assessment and actual assessment phases to determine recommendations.

These recommendations may include:

- Replace or upgrade existing hardware:
  - Replace shared-media Ethernet hubs with Layer 2 switching at a minimum
  - Utilize G.711 for LAN-based applications and G.729 for calls traversing the WAN. CODEC selection is based on overall objectives and cost targets for the VoIP deployment.
  - On links below 1.5 Mb, do not exceed 50 percent total peak loading
  - Make sure that delay does not exceed 150 ms. Packet loss should be less than 0.5 percent.
- Implement QoS:
  - Protocol prioritization
  - Traffic shaping (for Frame Relay)
  - Diffserve
  - IP fragmentation
  - Platform-queuing mechanisms
- Negotiate new network service contracts and service level agreements:
  - Availability
  - Call setup
  - Performance
  - Call Quality
  - Incident Tracking

Notes

Practice

Read each scenario. Describe the potential implementation issue the configuration presents and recommend the network improvement to insure a successful VoIP deployment.

1. The customer uses shared media access to connect to the WAN.

Issue:

Recommendation:

VLAN

Notes

2. All LAN traffic flows through a single device.

Issue:

Recommendation:

- VLAN
- UPS

3. The customer's service level agreement with its PSTN provider does not ensure any level of prioritization once the call enters the WAN.

Issue:

Recommendation:

Configure at entrance to PSTN.

4. The data network includes firewalls and Network Address Translation (NAT) devices to protect the network from unauthorized access.

Issue:

Recommendation:

Configuration firewall

5. The home office has a larger bandwidth connection than the remote sites.

Issue:

Recommendation:

IP [illegible]

6. A company wants to equip its regional sales personnel with soft IP clients. Most of the personnel use laptop computers.

Issue:

Recommendation:

Answers to Practice

If you successfully completed the Practice and are confident with your understanding of the material, then you have satisfied the lesson requirements.

Notes

Summary

In this lesson, you learned that planning is vital to successfully deploy a Voice over IP (VoIP) solution in an existing network. You learned about the recommended VoIP network assessment process and areas and the tools available to assist you with network assessment process. You also learned how to develop customer recommendations for network improvements, based on sample network assessment scenarios in preparation for VoIP deployment.

Notes